ICLG

The International Comparative Legal Guide to:

Cybersecurity 2019

2nd Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Angara Abello Concepcion Regala & Cruz Law Offices
Bagus Enrico & Partners
Boga & Associates
BTG Legal
Christopher & Lee Ong
Cliffe Dekker Hofmeyr Inc
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Ferchiou & Associés
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, S.P. R.L.
JIPYONG LLC
King & Wood Mallesons
Latham & Watkins LLP
Lee, Tsai & Partners Attorneys-at-Law
LT42 – The Legal Tech Company
Maples and Calder
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Simmons & Simmons LLP
Siqueira Castro Advogados
Stehlin & Associes
Synch
Templars
USCOV | Attorneys at Law

glg
global legal group

glg
global legal group

Contributing Editors
Nigel Parker & Alexandra Rendell, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Sam Friend

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
October 2018

ISBN 978-1-912509-38-6
ISSN 2515-4206

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

EDITORIAL

Welcome to the second edition of *The International Comparative Legal Guide to: Cybersecurity*.

This guide provides corporate counsel and international practitioners with a comprehensive worldwide legal analysis of the laws and regulations of cybersecurity.

It is divided into two main sections:

Three general chapters. These chapters are designed to provide readers with an overview of key issues affecting cybersecurity, particularly from the perspective of a multi-jurisdictional transaction.

Country question and answer chapters. These provide a broad overview of common issues in cybersecurity laws and regulations in 32 jurisdictions.

All chapters are written by leading cybersecurity lawyers and industry specialists and we are extremely grateful for their excellent contributions.

Special thanks are reserved for the contributing editors Nigel Parker and Alexandra Rendell of Allen & Overy LLP for their invaluable assistance.

Global Legal Group hopes that you find this guide practical and interesting.

The *International Comparative Legal Guide* series is also available online at www.iclg.com.

Alan Falach LL.M.
Group Consulting Editor
Global Legal Group
Alan.Falach@glgroup.co.uk

The Regulators Have Spoken – Nine Lessons To Help Protect Your Business

Nigel Parker

Alexandra Rendell

Allen & Overy LLP

Introduction

According to a 2018 survey by the UK Government's Department for Digital, Culture, Media and Sport[1] approximately four in 10 businesses reported a cyber breach or attack in the preceding 12 months. Almost 40 per cent of such incidents have resulted in financial or data loss.

Regulators are rightly placing an increasing focus on cybersecurity. For example, in 2017, in the US the New York State Department of Financial Services adopted a final regulation on cybersecurity requirements for financial services companies.[2] In the first half of 2018, the US Securities and Exchange Commission approved a statement and interpretive guidance on public companies' disclosure obligations regarding cybersecurity risks and incidents.

In the UK, in a recent speech at the National Cyber Security Centre's CYBERUK 2018 event, the UK Information Commissioner commented that the UK Information Commissioner's Office (**ICO**) now views cybersecurity as "the spine running through all [their] work".[3] The ICO has also updated its Information Rights Strategic Plan for 2017–2021[4] to add cyber incidents as a sixth strategic goal, and has published its first Technology Strategy for 2018–2021.[5] The Technology Strategy notes that the ICO will appoint a panel of forensic investigators to assist with regulatory work, and will publish an annual report on "lessons learned" from cyber breaches reported to the ICO and technology issues emerging from data protection impact assessments. The ICO has fined several organisations that have fallen victim to cyber attacks for failure to implement adequate security measures, and such fines are likely to rise significantly under the General Data Protection Regulation, which allows data protection authorities to levy fines of up to the higher of €20 million or four per cent of the annual worldwide turnover.

Regulatory enforcement action can provide helpful insight for organisations seeking to take steps to minimise the risk of a regulatory fine. In publishing enforcement decisions, regulators will typically (and may be required) to explain what a particular organisation did or, more often than not, failed to do, in breach of their legal and regulatory obligations. Regulators may also highlight positive steps taken by an organisation. In both cases, lessons can be learned from these statements.

Key Lessons From Data Protection Enforcement Examples

There are a number of lessons that can already be taken from previous cyber breaches that have resulted in enforcement action. In many cases, the failings highlighted reveal basic failures:

1. **Keep software up to date**. In January 2018, Carphone Warehouse was fined £400,000 by the ICO in relation to a 2015 data breach affecting a database containing information of over three million individuals. One of the factors contributing to the seriousness of the breach was that Carphone Warehouse was using software that was six years old at the time of the attack. Carphone Warehouse continued to use a WordPress installation dated from 2009, although more current versions were available. The ICO took the view that the age of the software made an attack more likely and easier to execute.[6] Similarly, when TalkTalk received its then-record £400,000 fine from the ICO in October 2016[7] in relation to a cyber attack that exploited vulnerabilities in historic webpages that allowed access to a database containing personal data of over 150,000 customers, one of the contributing factors highlighted in the ICO's monetary penalty notice was that the TalkTalk group was operating with outdated database software. In that instance, the ICO highlighted the use of an outdated version of the MySQL database management software. Companies should ensure that software used, particularly in core operating systems and databases, is up-to-date and supported.
2. **Promptly apply all required security patches**. In much the same way that software should be kept up to date, if a vulnerability is identified and a patch issued by the software supplier, ensure that the patch is applied in a timely manner. This was a particularly egregious failing in the case of TalkTalk's October 2016 data breach, where TalkTalk's already outdated MySQL software was affected by a bug for which a fix had been made available by the software vendor over three-and-a-half years before the cyber attack.[8] It was also a significant factor in a breach affecting Gloucester City Council, which failed to update software to implement a patch for the "Heartbleed" vulnerability in 2014.[9] In that case, the Council's IT staff identified the Heartbleed vulnerability, for which a new version of the affected software, OpenSSL, had already been made available to fix the flaw. The Council intended to apply the patch in accordance with its update policy, but was in the process of outsourcing its IT services to a third party and, during the course of the outsourcing process, overlooked the software patch. Most recently, in September 2018, the ICO issued a fine of £500,000 (the maximum allowed under the Data Protection Act 1998) to Equifax Ltd in relation to the 2017 cyber attack affecting Equifax Inc. in the US.[10] The attack exploited a vulnerability in a web application framework used by Equifax Inc., which was disclosed to Equifax Inc. by the US Department of Homeland Security Computer Emergency Readiness Team two months before the first evidence of the attack was recorded. The vulnerability was given a maximum score of 10.0, indicating a critical vulnerability requiring immediate attention, but Equifax Inc. failed to identify and patch the installation on its consumer-facing disputes portal, where the attack subsequently took place.

3. **Implement routine vulnerability scanning and penetration testing procedures**. SQL injection attacks and similar penetration attacks are reasonably common tools used by cyber attackers, and contributed to at least three attacks that resulted in recent ICO monetary penalties.[11] The ICO has regularly highlighted the need for routine penetration testing procedures as part of an organisation's cybersecurity toolkit. While such security measures will not prevent a sophisticated or determined attacker, the ICO's recent enforcement practices indicate that the lack of routine testing is an obvious deficiency that will only serve to increase regulatory risk to an organisation in the event of a breach.

4. **Implement a Web Application Firewall (WAF)** for monitoring and filtering HTTP traffic to and from web applications. The WAF is different from a regular firewall in that it is able to filter the content of specific web applications to protect servers, rather than merely act as a gateway between servers. In doing so, a WAF can help defend against DDoS attacks and SQL injection attacks, among others. In Carphone Warehouse's case,[12] the absence of a WAF was viewed as a "significant deficiency" and a "notable departure from widely accepted security standards".

5. **Implement security policies in practice, not just on paper**. Having policies and procedures in place in respect of cybersecurity is one thing, but organisations need to ensure that those policies and procedures are implemented in practice. Regulators are unlikely to look favourably on failures to follow policies in respect of basic, industry-standard security measures. This issue was highlighted specifically in the ICO's response to Carphone Warehouse,[13] where policies such as patch management standards and antivirus policies were in place, but were not being followed in practice and Carphone Warehouse had no measures in place to check whether its policies were being followed. As the Information Commissioner herself said, "these companies may have the best policies in the world – but if those policies are not enforced, and personal data sits on unpatched systems with unmanaged levels of employee access, then a breach is just waiting to happen".[14] The ICO also highlighted this point in its response to Equifax Ltd in September 2018,[15] where Equifax Ltd failed to store relevant consumer data in encrypted form, contrary to Equifax's applicable data handling standards.

6. **Ensure passwords are sufficiently complex**[16] and **not stored in plain text**. Password policies are ubiquitous, particularly in an age of flexibility, mobile working and connected devices, but care should be taken to ensure that they are followed and that default passwords are avoided. The UK National Cyber Security Centre has published password guidance to help organisations simplify their approach.[17] One of the recommendations in the guidance is never to store passwords as plain text. It is common for users to re-use passwords. An attacker who gains access to a database containing plain text passwords already knows a user's credentials for one system. The attacker could then use this information to attempt to gain access to more important accounts, where further damage can be done. This was another aggravating factor in the Carphone Warehouse data breach[18] where the encryption key for encrypted transaction data on the relevant system was stored in plain text within the application's source code, and so was easily accessible to the attacker once the system had been breached. The same applied in the Equifax Ltd cyber attack,[19] where the ICO rejected Equifax Ltd's argument that passwords were stored in plain text for the purposes of fraud prevention and password analysis as not being a valid reason for storing personal data in plain text. In that case, the ICO identified failings in permitting accounts to have more permissions than needed, including allowing staff to access plain text password files.

7. **Keep access to key systems and databases restricted to a minimum number of staff.**[20] This is particularly relevant in the case of administrator access to systems and databases. It is also relevant to third-party access. Many organisations focus on internal security measures and access, but it is imperative to take steps to mitigate third-party risk as well. Minimising access to key systems is one of the ways to help mitigate these risks. Staff access to systems should be justified on a "need to know" basis.

8. **Keep data to a minimum**. It is important not to retain excessive amounts of data, particularly excessive historical data or data such as credit card details relating to historic transactions.[21] Data minimisation is a key principle of data protection law – while no organisation will be able to prevent a determined cyber attacker, the risk and damage flowing from a cyber attack can be mitigated by taking steps to ensure that the volume of data that can be accessed is kept to the absolute minimum. One of the key factors in the £500,000 fine imposed by the ICO on Equifax Ltd was that relevant UK data, which was later compromised in the cyber attack, had been migrated from servers in the US to the UK prior to the attack, but was not subsequently deleted in full from the US servers even though it was no longer necessary for it to be stored in the US.[22]

9. **Be transparent**. The reputational impact of a cyber attack can be huge, and can call into question the quality and integrity of measures introduced to safeguard data. As such, it can be tempting to keep a breach under wraps for as long as possible. However, the data breach affecting Yahoo (now known as Altaba), in particular, illustrates the importance of transparency as a means to mitigate regulatory risk, and the reputational impact of remaining silent. In that case, the SEC imposed a fine of $35 million, the first ever against a public company for failure to disclose a cyber breach.[23] In December 2014, Yahoo suffered a massive breach of its user database resulting in the theft of hundreds of millions of its users' data. Yahoo discovered the breach within days, and Yahoo's Chief Information Security Officer notified the senior management and legal teams. However, Yahoo did not publicly disclose the breach until 2016, in connection with its acquisition by Verizon. In the intervening period, Yahoo had both failed to disclose the breach in its risk factor disclosures in annual and quarterly reports and in the due diligence process with Verizon. In total, all of Yahoo's three billion users were likely to be compromised. The SEC found that Yahoo violated various provisions of the US Securities Act and the US Exchange Act in respect of market disclosures and misleading investors. A couple of months before imposing that fine, the SEC had issued guidance on public company cybersecurity disclosures.[24] In particular, the guidance covers the need for a public company to address cybersecurity threats and the consequences of compliance in its disclosures, as well as the need to disclose and describe past cyber attacks. Separately, following the eventual disclosure of the breach, Yahoo also received a fine of £250,000 from the ICO for failure to take appropriate technical and organisational measures to protect data, in particular for failure to implement monitoring procedures to flag instructions to transfer large quantities of data from the servers on which they were held and place it in the control of unauthorised individuals.

   The transparency requirement is now addressed to a certain extent by the introduction of mandatory data breach reporting requirements under the GDPR. Personal data breaches must be reported to the relevant supervisory authority without undue delay and, where feasible, within 72 hours. Any delay, or any decision not to report a breach, must be justified and documented. Even absent the SEC order, in a post-GDPR world Yahoo would not have been able to hide such a significant data breach for the time that it did. It is therefore unlikely that other organisations will find themselves in a similar position to Yahoo, as to do so would risk fines under GDPR as well as under market disclosure rules.

For public companies in the UK, the UK Listing Authority, in contrast to the SEC, has not issued guidance that specifically addresses cybersecurity. However, UK-listed companies are required, under the Prospectus Rules, to include a comprehensive and specific description of risks relevant to the issuer, the industry in which it operates and the securities being offered or listed. These obligations are broad enough to capture the disclosure of cybersecurity threats. Similarly, under the Companies Act 2006 and the Disclosure and Transparency Rules (**DTRs**), UK-listed companies should describe the principal risks and uncertainties facing the company, which could also cover cyber risk, both past and future. Finally, the existence of a cyber attack may amount to inside information requiring disclosure under the DTRs, as well as potentially triggering a UK-listed company's general obligation under the Market Abuse Regulation to notify the market as soon as possible of any inside information.

In an interesting counter example, the data breach affecting Morrisons in 2014 gives some insight into positive findings of good cybersecurity and data protection practices, and demonstrates that Morrisons had implemented some of the measures outlined in this article. In that case, a Morrisons employee deliberately published a file containing details of 99,998 Morrisons employees on a file sharing website, and later anonymously sent the data to three UK newspapers. The data included names, addresses, phone numbers, bank account details and salary details of the relevant employees. The individual responsible for this attack was employed in a senior internal audit role and had access to the data in accordance with that role. He was subsequently sentenced to eight years' imprisonment for offences under the Computer Misuse Act 1990 and the Data Protection Act 1998. In his judgment,[25] Langstaff J found that Morrisons had no primary liability for the breach of its security obligations as a data controller under the Data Protection Act 1998. In particular, Langstaff J found that Morrisons had appropriate internal policies, including an employee handbook, in place alerting employees to their obligations and to the fact that Morrisons would monitor communications to detect and investigate a breach of its policies. Langstaff J also noted that Morrisons had an external-facing firewall connected directly to the internet, coupled with a second firewall that protected Morrisons' internal network. An intrusion detection system was in place to detect patterns which might indicate a potential external attack. Although Morrisons faced civil claims from the affected employees in the courts, both the ICO (which did not impose any sanction on Morrisons following a lengthy investigation into this breach) and the court found that Morrisons had taken all steps to meet its legal and regulatory obligations.

Regulators recognise that it may not be possible to prevent a determined attacker, but will not look kindly on an organisation that fails to take the most basic preventative steps. Implementing the above measures may not fully eradicate risks but they certainly strengthen protections and will serve to mitigate any enforcement action from regulatory authorities, as well as minimising reputational damage.

Endnotes

1. UK Government Department for Digital, Culture, Media and Sport, *Cyber Security Breaches Survey 2018: Statistical Release* (2018).
2. https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.
3. UK Information Commissioner speech to CYBERUK 2018, *Building the cyber security community*, 12 April 2018.
4. https://ico.org.uk/media/about-the-ico/documents/2014134/20170413icoinformationrightsstrategicplan2017to2021v10.pdf.
5. https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf.
6. Carphone Warehouse, January 2018 (https://ico.org.uk/media/action-weve-taken/mpns/2172972/carphone-warehouse-mpn-20180110.pdf).
7. TalkTalk, October 2016 (https://ico.org.uk/media/action-weve-taken/mpns/1625131/mpn-talk-talk-group-plc.pdf).
8. TalkTalk, October 2016 (https://ico.org.uk/media/action-weve-taken/mpns/1625131/mpn-talk-talk-group-plc.pdf).
9. Gloucester City Council, May 2017 (https://ico.org.uk/media/action-weve-taken/mpns/2014217/gloucester-city-council-mpn-20170525.pdf).
10. Equifax Ltd, September 2018 (https://ico.org.uk/media/action-weve-taken/mpns/2259808/equifax-ltd-mpn-20180919.pdf).
11. Carphone Warehouse, January 2018 (https://ico.org.uk/media/action-weve-taken/mpns/2172972/carphone-warehouse-mpn-20180110.pdf); Boomerang Video, June 2017 (https://ico.org.uk/media/action-weve-taken/mpns/2014300/mpn-boomerang-video-ltd.pdf); Construction Materials Online Ltd, May 2017 (https://ico.org.uk/media/action-weve-taken/mpns/2013981/mpn-construction-materials-online-ltd-20170426.pdf).
12. Carphone Warehouse, January 2018 (https://ico.org.uk/media/action-weve-taken/mpns/2172972/carphone-warehouse-mpn-20180110.pdf).
13. Carphone Warehouse, January 2018 (https://ico.org.uk/media/action-weve-taken/mpns/2172972/carphone-warehouse-mpn-20180110.pdf).
14. UK Information Commissioner speech to CYBERUK 2018, *Building the cyber security community*, 12 April 2018.
15. Equifax Ltd, September 2018 (https://ico.org.uk/media/action-weve-taken/mpns/2259808/equifax-ltd-mpn-20180919.pdf).
16. Boomerang Video, June 2017 (https://ico.org.uk/media/action-weve-taken/mpns/2014300/mpn-boomerang-video-ltd.pdf); Construction Materials Online Ltd, May 2017 (https://ico.org.uk/media/action-weve-taken/mpns/2013981/mpn-construction-materials-online-ltd-20170426.pdf).
17. https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach.
18. Carphone Warehouse, January 2018 (https://ico.org.uk/media/action-weve-taken/mpns/2172972/carphone-warehouse-mpn-20180110.pdf).
19. Equifax Ltd, September 2018 (https://ico.org.uk/media/action-weve-taken/mpns/2259808/equifax-ltd-mpn-20180919.pdf).
20. Carphone Warehouse, January 2018 (https://ico.org.uk/media/action-weve-taken/mpns/2172972/carphone-warehouse-mpn-20180110.pdf); TalkTalk, August 2017 (https://ico.org.uk/media/action-weve-taken/mpns/2014626/mpn-talktalk-20170807.pdf).
21. Carphone Warehouse, January 2018 (https://ico.org.uk/media/action-weve-taken/mpns/2172972/carphone-warehouse-mpn-20180110.pdf).
22. Equifax Ltd, September 2018 (https://ico.org.uk/media/action-weve-taken/mpns/2259808/equifax-ltd-mpn-20180919.pdf).
23. https://www.sec.gov/litigation/admin/2018/33-10485.pdf.
24. https://www.sec.gov/rules/interp/2018/33-10459.pdf.
25. https://www.judiciary.uk/wp-content/uploads/2017/12/morrisons_approved_judgment.pdf.

Nigel Parker
Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: *+44 203 088 3136*
Email: *nigel.parker@allenovery.com*
URL: *www.allenovery.com*

Nigel is a partner specialising in intellectual property, data protection and privacy, commercial contracts and IT law. He is a member of the firm's Cyber Security Group and has advised clients on strategies for managing legal risk in relation to cybersecurity, including the deployment of a variety of risk management tools, on the response to attacks and dealing with regulatory authorities, and on taking pro-active steps in response to attacks.

Chambers 2015 cites Nigel as an expert in the fields of data privacy and outsourcing, describing him as "technically faultless" as well as "very practical and very good at finding solutions".

Alexandra Rendell
Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: *+44 203 088 2639*
Email: *alexandra.rendell@allenovery.com*
URL: *www.allenovery.com*

Alexandra is an associate specialising in commercial contracts, data protection, intellectual property and information technology law. Alexandra advises on complex commercial arrangements for a range of clients in the technology and financial services sector, including outsourcing and service provision arrangements, licensing and IP/data exploitation.

ALLEN & OVERY

Allen & Overy is a full-service global elite law firm headquartered in London. Our commitment to help our clients deliver their global strategies has seen us build a truly global network now spanning 44 offices in 31 countries. We have also developed strong ties with relationship law firms in more than 100 countries where we do not have a presence.

We have a strong cybersecurity practice comprising a core team of 15 partners with diverse backgrounds in data protection, bank regulation, antitrust, securities laws, technology, IT, litigation, employment, IP and corporate. This spread is crucial because cybersecurity incidents frequently span a wide range of traditional legal practice areas. There is an important legal component to cybersecurity and our integrated team of diverse practitioners reflects this requirement. As a full-service global elite law firm, we are able to advise clients on all legal issues concerning cybersecurity.

Cybersecurity and Digital Health: *Diabolus ex Machina*?

Paolo Caldato

David Fitzpatrick

Simmons & Simmons LLP

1 Introduction

In July 2018, Singapore experienced its most severe cyber-attack to date. Hackers targeted the city-state's largest healthcare group, copying the personal data of 1.5 million patients[1] and leaking the details of medicine dispensed to about 160,000 people, including the Prime Minister.[2] While few attacks have taken place on such a grand scale, this is by no means an isolated incident, and the evidence suggests that the incidence of further attacks on the healthcare industry will accelerate.[3]

The adoption by healthcare organisations and consumers of the Internet of Things, cloud-based services and "big data" analytics is now the norm.[4] A key feature of this new landscape has been the explosion of mHealth apps and other digital health technologies on the market (and in the pipeline). These products push the boundaries of innovation, and enable an enhanced and more efficient healthcare delivery service that does not operate exclusively within large healthcare organisations but is available at consumers' fingertips. This promises to transform and disrupt how consumers access medical services and receive (and take responsibility for) bespoke healthcare in the developed world, and has already allowed medical technology to leap-frog traditional infrastructure challenges in Africa.

Digital health has also revolutionised the collection and processing of personal medical data, particularly in terms of the categories and volumes of data being collected. The analytical possibilities offered by the availability of these data, and their consequent socio-medical applications, are endless and promise very real opportunities for consumers to receive personalised, real-time healthcare services that could materially reduce the cost for national health services of treating chronic and lifestyle diseases and associated medical complications.

However, with the increased availability of data comes both increased interest in stealing those data and increased vulnerability to attempts to do so. Despite the pressing need for effective defences against cybersecurity breaches, many of these innovations are not sufficiently well-equipped to withstand the tide of attacks on the horizon; in many cases, the issue of cybersecurity is relegated to an afterthought. This has led to medical devices (including digital health technology) being described as "the next security nightmare".[5]

In order to play catch-up with this new technological reality, the European Union has introduced a raft of new regulation over the past two years. In reality, much of this is intended to address other subjects, and at times, references to cybersecurity remain few and far between, and difficult to pinpoint. That said, it is undeniable that the regulatory burden on companies engaged in digital health has increased, and will continue to do so; in this respect, neglect of cybersecurity goes far beyond a major hindrance to service delivery, but can be the catalyst for potentially crippling fines, unwelcome litigation and, ultimately, reputational meltdown.

These difficulties can leave potential investors in these technologies with a headache: any up-side in investing will not be predicated solely on product quality or innovation, but also on the robustness of the company commercialising the product or innovation in question, and its ability to prevent, and (perhaps more realistically) reduce the impact of, cybersecurity incidents.

2 The Vulnerability of Medical Devices

Digital health technology has rapidly evolved in recent years: non-networked and isolated equipment has quickly made way for fully-fledged networked equipment with features such as remote access, wireless connectivity and pre-installed software, used widely both within healthcare organisations and by consumers at home. Often, this technology is connected to smart devices, such as mobile phones and tablets. Wearable devices incorporating medical apps and software are also on the rise. Increasingly, these products require personal data to function. However, vulnerabilities are not limited to data leaks; in the most extreme cases, hacks can give access to other networks, install ransomware or achieve control of the device itself.

These concerns have played out in practice and have the potential to be life-threatening. In October 2016, Johnson & Johnson warned its patients that a security vulnerability in its networked insulin pumps could potentially enable hackers to administer insulin overdoses to diabetic users.[6] In August 2017, around 465,000 of St Jude Medical's pacemakers were recalled by the U.S. Food and Drug Administration (the "FDA") owing to concerns over their connections to mobile devices and diagnostic systems that left them vulnerable to tampering.[7] Such concerns were not lost on former U.S. Vice President, Dick Cheney, who asked that his doctors modify his heart defibrillator so as to thwart its vulnerability to hacking.[8]

Often, it is not large, established organisations well-versed in risk and regulation that are behind these products. Instead, they are frequently conceived, marketed and supported by start-ups, who may be tempted (or financially compelled) to forgo the integration of security mechanisms in order to expedite the launch of their products onto a fast-moving market. Although coding errors, insecure protocols, out-of-date software and password flaws remain possible, product quality and associated patient care issues, rather than security, are likely to be their primary concerns. This is reflected in much of the regulation that governs medical devices, which contains no shortage of information on matters concerning patient health, but offers sparse detail to address the prevention, and remediation, of cybersecurity breaches.

Clearly, these difficulties present fertile ground for hackers, who employ all manner of tactics, such as spoofing or impersonation, social engineering, phishing, and malicious code, in order to compromise medical devices. A current phenomenon is the use by criminals of malware to encrypt information before demanding payment via digital currency to recover the information (including patient records). And, of course, there is always the risk of a data breach being committed by a disgruntled employee with access to sensitive information.

3 Regulatory Framework

The regulatory framework that governs the security of medical devices in the European Union is patchwork in nature and lags behind the US regime, where the FDA has issued several pieces of guidance on the issue that directly address cybersecurity.[9] This disparity is, in no small part, due to the fact that current European regulations tend to focus on patient safety but contain very few direct references to cybersecurity risk. Furthermore, no single set of standards can be found in one place, but must be filtered through three separate lenses: (i) regulations in relation to medical devices; (ii) cybersecurity-specific regulation; and (iii) data protection regulation. Cognisant of the need for regulation to catch up with the exponential increase in new technologies, the EU has been legislating in each of these three fields. As a result, cybersecurity can no longer tenably be considered an issue that permits a reactive approach; instead proactive engagement will be required from stakeholders throughout a product's supply chain and lifespan.

Medical Devices Regulation

The European Parliament recently conducted a comprehensive revision of European legislation of medical devices, pursuant to which, amongst other things, the Medical Devices Directive[10] and the Active Implantable Medical Devices Directive[11] are being phased out and replaced by a new Medical Devices Regulation (the "MDR").[12] The MDR entered into force on 25 May 2017, with a transitional period of three years.[13]

The Medical Devices Directive, as amended, already confirmed that software in its own right can fall under the definition of medical device, where the software is intended by the manufacturer to be used for the purpose of:

(i) diagnosis, prevention, monitoring, treatment or alleviation of disease;

(ii) diagnosis, monitoring, treatment, alleviation or compensation for an injury or handicap;

(iii) investigation, replacement or modification of the anatomy or of a physiological process; or

(iv) control of conception.

The MDR expands this definition to include devices used for the "prognosis" and "prediction" of diseases[14] and, by association, their accessories (that is, articles intended by manufacturers to be used in accordance with the device's purpose or to assist its functionality).[15] A list of product groups that, despite having no intended medical purpose (notably, products introduced into the body via surgically invasive means in order to modify anatomy, and equipment using electrical or magnetic currents to stimulate the brain) will also be treated as medical devices,[16] and the European Commission has reserved the right to add new groups by means of delegated acts.[17] However, the MDR stops short of including in the definition software intended for general purposes, such as lifestyle and well-being apps. While there are sure to be grey areas, this broader definition presents challenges for an exponentially growing market; what a manufacturer may consider to be the latest home-health gadget could actually transpire to be a medical device that requires strict regulatory compliance (including in relation to cybersecurity) in order to be commercialised legally.

The MDR goes further than previous legislation in its explicit reference to cybersecurity. It requires devices to be designed and manufactured in such a way as to: (i) remove or reduce as far as possible the risks associated with the possible negative interaction between software and the IT environment with which it operates and interacts;[18] and (ii) protect against unauthorised access that could hamper the device from functioning as intended.[19] Manufacturers are also required to set out minimum requirements concerning hardware, IT network characteristics and IT security measures, including protection against unauthorised access.[20]

General Data Protection Regulation

The General Data Protection Regulation (the "GDPR"),[21] which came into force on 25 May 2018 and is supplemented in the UK by the Data Protection Act 2018 (the "DPA"),[22] requires data controllers to comply with six data protection principles[23] with respect to personal data (a broad concept that encompasses any information, including health data, that can be used to identify an individual).[24] The sixth data principle states:

> "*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisation measures.*"[25]

While much GDPR-related discussion in the healthcare industry has centred on the issues of the collection, storage and use of patient data, and associated consent, the GDPR increases the demands on healthcare organisations and app developers from a cybersecurity perspective: both data controllers *and* processors are required to implement security measures that are appropriate, taking into account factors such as data type, the nature and purpose of processing, the risk to individual rights associated with any security breach and the costs of implementation.[26] The following examples are given in the legislation: (i) anonymisation (or "pseudonymisation")[27] and encryption; (ii) ensuring the ongoing confidentiality, integrity, availability and resilience of the systems that process the data; (iii) the ability to restore access in a timely manner following an incident; and (iv) a process to test, access and evaluate the effectiveness of those security measures.[28]

Personal data breaches must be notified by data processors to data controllers, and by data controllers to the relevant supervisory authority (in the UK, the Information Commissioner's Office (the "ICO")) without undue delay.[29] In the case of data controllers, this notification should, where feasible, take place within 72 hours of the data controller becoming aware of the breach, but no notification need take place if the breach is unlikely to result in a risk to the rights and freedoms of natural persons.[30] Where such a risk is high, however, the data controller must, without undue delay, notify the data subjects of the personal data breach, unless: (i) appropriate technical and organisational protection measures were applied to the data affected by the breach; (ii) the data controller has taken subsequent measures to ensure that the risk to rights and freedoms of data subjects is no longer likely to materialise; and (iii) it would involve disproportionate effort (in which case, there would instead be a public communication or similar measure whereby the data subjects would be informed in an equally effective manner as that prescribed by the notification requirements).[31] Breaches are not to be taken lightly and can lead to fines of up to 4% of global annual turnover.[32]

NIS Directive

Comparatively little attention has been given to the EU Directive on the Security of Networks and Information Systems (the "NIS Directive"),[33] which is often referred to as "the Cybersecurity Directive". The NIS Directive was implemented in the UK on 10 May 2018 by the Network and Information Systems Regulations 2018 (the "NIS Regulations"). The NIS Directive subjects operators of essential services ("OESs"), such as healthcare providers, and relevant digital service providers ("RDSPs"), including cloud computing services, to additional risk management and reporting requirements.[34] A myriad of medical devices and digital health apps fall under the scope of the NIS Directive by virtue of constituting network and information systems under the terms of the legislation.[35]

In the UK, the NIS Regulations favour broad outcome-based principles over prescriptive rules. The National Cyber Security Centre (the "NCSC") has published four top-level objectives for OESs (under which sit 14 high-level compliance principles). These are: (i) managing security risk; (ii) defending systems against cyber-attacks; (iii) detecting cybersecurity events; and (iv) minimising the impact of cybersecurity incidents.

OESs are required to report any incident that "has a significant impact on the continuity of the essential service which that OES provides",[36] while RDSPs must report "any incident having a substantial impact on the provision of any of the digital services [that applies]".[37] Reporting timeframes mirror those in the GDPR, in that notification to the relevant competent authority[38] must take place "without undue delay" and no later than 72 hours after the OES or RDSP becomes aware of the incident.[39] Relevant competent authorities are empowered to monitor compliance with security and notification duties by conducting, or ordering, inspections (the reasonable costs of which will be borne by the relevant OES or RSDP).[40] The most serious breaches of the NIS Regulations can leave a company liable for a fine of £17,000,000.[41]

Although the NIS Directive and the GDPR are products of different EU concerns (the former is intended primarily for companies that are involved in providing critical infrastructure services, while the latter addresses all organisations that process personal data) there is a considerable degree of overlap between the Regulations as they pertain to cybersecurity. For example, if a digital health provider or healthcare organisation were hacked, both the personal data that it holds (in respect of which the GDPR would apply) and its service delivery (in respect of which the NIS Directive would apply) would likely be compromised.

4 Breach and Liability

A business that has fallen victim to a cybersecurity breach will have to invest substantial sums in internal remediation measures, which will require a full exploration of the breach, as well as of the proposed measures to contain, and eradicate, the threat and the steps to ensure that the system is future-proofed against similar attacks. However, a breach can have an impact far beyond the immediate aftermath and remediation process: large regulatory fines, litigation and reputational damage are very real prospects. It is, therefore, important for investors to consider these risks and assess where liability may lie in the event of a breach.

ICO fines

The ICO has had the power to issue fines for failures to follow security obligations from as early as 2010. These fines were linked regularly to breaches of the seventh data protection principle (often in connection with other principles) under the Data Protection Act 1998,[42] the wording of which (much like that in the GDPR's sixth principle) required:

> *"…appropriate technical and organisational measures… against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

For example, in February 2017, the ICO fined private health company, HCA International Ltd, £200,000 for its failure to safeguard the confidential personal information of fertility patients.[43]

It remains to be seen how enforcement action will look in the post-GDPR climate. The severity of the sanctions now available to the ICO, coupled with an increase in the ICO budget for 2018/2019 from £24 million to £34 million (partly owing to the need for more enforcement officers),[44] might suggest that higher fines will become the norm. Indeed, in one of its first instances of enforcement action following the entry into force of the GDPR, the ICO penalised Facebook with the maximum available fine under the Data Protection Act 1998 of £500,000 (and noted that the sum would have been more hard-hitting had the breaches occurred after the commencement of the GDPR on 25 May 2018) for the social media titan's role in the Cambridge Analytica scandal, which resulted in the harvesting of, allegedly, 50,000,000 user profiles. Some experts consider this to be a warning shot from the ICO and an indication that future enforcement action will have more teeth than previously was the case.[45] Such assertions may, however, be premature: the ICO has indicated that it has "no intention of changing the ICO's proportionate and pragmatic approach" and that "hefty fines will be reserved for those organisations that persistently, deliberately or negligently flout the law". Whichever view one takes, the digital health industry should pay particular attention to the ICO's intended focus on large-scale data and cybersecurity breaches involving sensitive information.[46]

Civil litigation

Irrespective of whether or not regulatory action has been taken, digital health companies remain vulnerable to court claims as a result of cybersecurity attacks involving their products. Under English law, claims may be brought pursuant to various causes of action, such as: (i) tortious misuse of private information; (ii) tortious or contractual breach of confidence; (iii) breach of a contractual term (express or implied) that customer data will be stored securely and with due care; (iv) tortious or contractual negligence, for a failure to take reasonable security precautions when storing customer information; and (v) under Article 82 of the GDPR for damage caused by a breach of the GDPR, and/or under section 169 of the DPA for a breach of data protection legislation, in the form of a compensation claim against the defendant data controller and/or processor.

Traditionally, UK cybersecurity cases have occupied little court time, largely owing to the uncertainty surrounding whether or not individuals have suffered damage (and, if so, how to quantify it). Claims made, or threatened, against businesses for a breach of the Data Protection Act 1998 were often low-value, and alleged offenders tended to opt for confidential settlements over the prospect of a PR disaster.

The GDPR may signal the dawn of a more litigious culture in healthcare, at least in relation to breaches involving personal data. Whereas previously, consumers may have been kept in the dark as to a breach, the new self-reporting requirements mean that they will now be notified of a breach at the same time as the regulatory authority; large regulatory fines may encourage "knock-on" litigation (or even motivate particularly vexed consumers to bring claims during the ICO's enforcement process).

Prohibitively expensive claims may also become less of an issue: data subjects are now entitled to appoint certain non-profit bodies to lodge a complaint on their behalf and exercise their right to compensation,[47] which could enable groups of claimants to be brought together through, for example, group litigation orders. Although the GDPR is very much in its infancy, it is not difficult to imagine opportunistic claims management companies heavily advertising the possibility of knock-on litigation following major data breaches. Furthermore, whilst pecuniary loss was formerly a prerequisite, the GDPR confirms the Court of Appeal's decision in *Vidal-Hall et al v Google*[48] that "damage" caused to consumers by data controllers and processors can include emotional distress alone; the terminology used in the GDPR is "material" or "non-material" damage.[49]

Contracts may also provide a basis for further liability in the event that a business's cybersecurity systems are compromised, although the relevant contractual nexus (and therefore, where that liability lies) will be heavily dependent on the way in which the product is delivered to, and operated in, the market. Where digital health companies not only design and manufacture products, but also support or run those products as third-party service providers for healthcare organisations, they may face claims for termination or contractual damages, pursuant to data protection clauses that have been breached as a result of cybersecurity failures. Consideration should also be given to any misrepresentations made to healthcare organisations, direct customers, or other third parties, as to the robustness of the app's cybersecurity systems. Such statements may have made their way into, for example, responses to RFPs, or prospectuses or marketing materials (as well as, of course, contractual documentation), and could result in misrepresentation claims by shareholders, suppliers, customers, or even investors.

Irrespective of whether or not the cybersecurity incident in question causes a data breach, in the absence of enforceable contractual restrictions on liability, claims can arise where the disruption to a business caused by a cybersecurity incident leaves the business unable to fulfil other contractual duties owed to its business counterparts.

Investors considering board seats after the acquisition of a digital health company should also be aware that they themselves may be potentially exposed to creative consumer claims, most likely for alleged breaches of fiduciary duties under the Companies Act 2006. Attempts could be made, for example, to argue that a failure to mitigate, and remedy, a cybersecurity incident constitutes a breach of a director's duty to promote the success of the company,[50] and/or to exercise reasonable skill and diligence in the conduct of his role, which, if made out, could give rise to personal liability on the part of the director.[51] Furthermore, and although it is no easy task to pierce the corporate veil and establish personal liability, that same creative claimant might attempt to fix a shareholder that was not on the board but was nonetheless active in the management of (or could be shown to be particularly knowledgeable about the business of) the digital health company with liability in respect of any such consumer claim.

Even if litigation does not materialise, where customer data have been compromised, companies can find themselves feeling pressure to offer to their customers significant *ex gratia* goodwill payments in order to mitigate any damage that the breach has caused to the customer relationship. And, of course, additional pressure to reach such an accommodation (on a confidential basis) is likely to arise from the fact that consumers (particularly those within patient groups) are heavily active on social media, and awareness of a successful claim is consequently likely to spread rapidly (and thereby generate copy-cat claims).

Whatever the nature and basis of a potential dispute, investors should be live to the fact that litigation is uncertain, and even where claims asserted are meritless, they still require time and money to be properly defended, and can lead to the business in question being irreparably damaged from a PR perspective.

5 Practicalities

Any consideration of an investment in a digital health entrepreneur should not be predicated solely on product quality. The investment decision should be influenced by a deep understanding of the business through which it is commercialised, or supplied to consumers or healthcare organisations. Ultimately, even the most innovative product on the market is likely to fail (and destroy any investment value) if it is commercialised in a way that leaves it vulnerable to significant losses, including through a failure to pay due regard to cybersecurity and the consequences of a data breach. The principal means of mitigating against this is proper due diligence, including a thorough understanding of the technology's genesis, purpose and method of operation, and an assessment of the business's ability to meet the regulatory requirements outlined above.

There is no shortage of resources available for those trying to navigate the complex issues that cybersecurity threats pose to investment in this sphere. Various guidance has been published by organisations such as the NCSC[52] and the British Standards Institution, the latter of which has published a paper that directly addresses the cybersecurity of medical devices.[53] Lessons can also be taken from the more developed US model.

As a guide, we set out below a (by no means exhaustive) checklist of relevant overarching considerations, divided into four categories: (i) risk assessment; (ii) contract; (iii) business culture; and (iv) incident response. It seems likely that, owing to the nature of digital health entrepreneurs, investors will have to be prepared to bring to the table ready-made solutions to these issues, rather than expecting a small digital health company with little experience, manpower or interest in commercial matters beyond innovation, to be market-ready on its own. Investors should, as with any potential investment, exercise a healthy sense of scepticism when weighing the opportunity, and should not be distracted from detailed enquiries by, for example, grandiose assurances about the product's robustness and commercial promise, and/or an eye-catching and high-profile set of non-executive directors (particularly where those directors are not themselves subject-matter experts).

Perhaps the best overarching question that one can ask in respect of a potential investment target is "would I honestly be willing to entrust my own most sensitive and valuable secrets to this company?". The checklist below is designed as a starting-point to assist with answering that fundamental question.

Acknowledgment

The authors should like to thank Robert Allen, a partner at Simmons & Simmons LLP, for his support with and input into this article, particularly on the parts requiring data protection expertise.

Risk assessment	How strong is the business's network(s) and IT security?
	What consideration has been given to cybersecurity during product development?
	Has product testing been carried out, including in appropriate "live" operational environments?
	Does the product/business rely on any third-party performance?
Contract	How does the business routinely contract around, and out of, its commercial risks?
	How are cybersecurity risks limited or apportioned in the contract?
	What is carved out of liability?
	What representations as to security have been given?
	Does the contract counterparty have the financial substance to stand behind its contractual commitments (and to satisfy any damages award against it), and how difficult would it be to enforce those contractual commitments against it?
Business culture	What are the business's security practices like?
	How are passwords distributed within the business?
	What information control policies are in place, and how are these implemented, enforced and periodically reviewed?
	Are employees aware of their personal security responsibilities?
	What auditing is performed in relation to use of/access to/restrictions on/tracking of cloud and other external storage systems?
	Is there regular training on regulatory requirements and security awareness?
Incident response	What incident management and crisis recovery/business continuity policies are in place?
	Is there an incident response team?
	Can the business co-operate with regulators' requests for information and/or access to data?
	Is there appropriate insurance in place to deal with a cybersecurity threat?

Endnotes

1. Around one quarter of the city-state's population.
2. Financial Times, "*Singapore prime minister among 1.5m patients affected by data hack*" (July 2018), available at https://www.ft.com/content/104aa8ec-8c03-11e8-b18d-0181731a0340.
3. In 2017, Cybersecurity Ventures predicated that global healthcare cybersecurity spending would exceed $65 billion cumulatively from 2017–2021 and that ransomware attacks on healthcare organisations would quadruple by 2020 (see Cybersecurity Ventures, "*Healthcare Security $65 Billion Market*" (April 2017), available at https://cybersecurityventures.com/healthcare-cybersecurity-report-2017/).
4. British Standards Institute, "*Cybersecurity of medical devices: Addressing patient safety and the security of patient health information*" (2017), authored by Richard Piggin, Security Consultant (Atkins), available at https://www.bsigroup.com/LocalFiles/EN-AU/ISO%2013485%20Medical%20Devices/Whitepapers/White_Paper___Cybersecurity_of_medical_devices.pdf.
5. Wired, "*Medical Devices are the Next Security Nightmare*" (March 2017), available at https://www.wired.com/2017/03/medical-devices-next-security-nightmare/.
6. Reuters, "*J&J warns diabetic patients: Insulin pump vulnerable to hacking*" (October 2016), available at https://uk.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e/jj-warns-diabetic-patients-insulin-pump-vulnerable-to-hacking-idUKKCN12411L.
7. ZDNet, "*FDA issues recall of 465,000 St. Judge pacemakers to patch security holes*" (August 2017), available at https://www.zdnet.com/article/fda-forces-st-jude-pacemaker-recall-to-patch-security-vulnerabilities/.
8. CNN, "*Cheney's defibrillator was modified to prevent hacking*" (October 2013), available at https://edition.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/index.html.
9. Available at https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm.
10. Council Directive 93/42/EEC of 14 June 1993 concerning medical devices.
11. Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices.
12. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices.
13. The MDR will be fully applicable on 26 May 2020. During the transition period, devices can be placed on the market under the current EU Directives, or the new Regulation (if the devices comply fully with the new Regulation) (https://www.gov.uk/guidance/medical-devices-eu-regulations-for-mdr-and-ivdr).
14. MDR, Article 2(1).
15. MDR, Article 2(2).
16. MDR, Annex XVI.
17. MDR, Article 1(5).
18. MDR, Annex I, 14.2.
19. MDR, Annex I, 18.8.
20. MDR, Annex I, 17.4.
21. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
22. The Data Protection Act 1998 has now been repealed and replaced.
23. GDPR, Articles 5(1) and (2).
24. GDPR, Article 4(1). The GDPR defines "data concerning health" as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status" (GDPR, Article 4(15)).

25. GDPR, Article 5(1)(f).
26. GDPR, Article 32(1).
27. Defined as "*…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*" (GDPR, Article 4(5)).
28. GDPR, Article 32(1).
29. GDPR, Article 33.
30. GDPR, Article 33.
31. GDPR, Article 34.
32. For some breaches (including failing to comply with the conditions for processing) data controllers can receive a fine of up to the greater of 4% of global annual turnover for the preceding year (for undertakings) or €20,000,000 (Article 83(5)). For a failure to comply with security obligations, the fine can be up to the greater of 2% of global annual turnover for the preceding year (for undertakings) or €10,000,000 (GDPR, Article 83(4)).
33. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
34. The security and notification requirements do not apply to RDSPs that employ fewer than 50 people, and whose annual turnover and/or balance sheet is less than €10,000,000 (NIS Directive, Article 16(11)).
35. The definition includes: (i) any electronic communications network (as defined under certain EU legislation); (ii) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (iii) digital data stored, processed, retrieved or transmitted by elements covered under (i) or (ii) for the purpose of their operation, use, protection and maintenance (NIS Directive, Article 4(1)).
36. NIS Regulations, Article 11(1).
37. NIS Regulations, Article 12(3).
38. There is no single competent authority; Schedule 1 to the NIS Regulations contains a list of designated competent authorities for particular sectors and sub-sectors.
39. NIS Regulations, Articles 11(3)(b)(i) and 12(6)(a).
40. NIS Regulations, Article 16.
41. NIS Regulations, Article 18(6)(d). This is for a material contravention that the enforcement authority determines has caused, or could cause, an incident resulting in an immediate threat to life or significant adverse impact on the United Kingdom economy. It is understood that a "double jeopardy" scenario will not apply to an incident that breaches both the NIS Regulations and the GDPR, and that a company will only be fined under one of the Regulations, unless the penalties relate to different aspects of the wrongdoing and different impacts (see the government's response to public consultation, "*Security of Network and Information Systems*" (January 2018), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf).
42. In the UK, this implemented Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
43. ICO, "*Private health firm fined £200,000 after IVF patients' confidential conversations revealed online*" (February 2017), available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/02/private-health-firm-fined-200-000-after-ivf-patients-confidential-conversations-revealed-online/.
44. RSM UK, "*Information Commissioner sets out expectations for GDPR enforcement post 25 May 2018*" (25 May 2018), available at https://www.rsmuk.com/ideas-and-insights/information-commissioner-sets-out-expectations-for-gdpr-enforcement-post-25-may-2018.
45. Digiday UK, "*'It's a warning shot': Experts say ICO's fine to Facebook signals seriousness of its GDPR enforcement*" (16 July 2018), available at https://digiday.com/media/warning-shot-experts-say-icos-fine-facebook-signals-seriousness-gdpr-enforcement/.
46. ICO, "*Regulatory Action Policy*" (May 2018), available at https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
47. GDPR, Article 80.
48. [2015] EWCA Civ 311.
49. GDPR, Article 82.
50. Companies Act 2006, s172.
51. Companies Act 2006, s174.
52. See, for example, NCSC, "*10 Steps to Cyber Security*" (August 2016), available at https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.
53. Piggin, *Cybersecurity of medical devices*.

Paolo Caldato
Simmons & Simmons LLP
CityPoint
One Ropemaker Street
London EC2Y 9SS
United Kingdom

Tel: +44 20 7825 4621
Email: paolo.caldato@simmons-simmons.com
URL: www.simmons-simmons.com

Paolo is a Managing Associate in the Commercial Litigation group in Simmons & Simmons LLP's London office. His primary focus is on high-tech disputes in the Healthcare & Life Sciences and TMT sectors. Much of Paolo's work involves cross-border litigation for international clients. Paolo's first degree was in the biological sciences (with honours in biochemistry). He is a member of the firm's International Digital Health team, and the Society for Computers and Law. He is also a Tech London Advocate (in the TLA's Health Tech working group), and sits on the Legal Issues and Compliance Committee of the Association of British HealthTech Industries.

David Fitzpatrick
Simmons & Simmons LLP
CityPoint
One Ropemaker Street
London EC2Y 9SS
United Kingdom

Tel: +44 20 7825 5784
Email: david.fitzpatrick@simmons-simmons.com
URL: www.simmons-simmons.com

David is an Associate in the Commercial Litigation group in Simmons & Simmons LLP's Bristol and London offices. He acts for clients on a range of corporate and commercial disputes, often with an international focus and in the Healthcare & Life Sciences and TMT sectors. He has been published on a number of platforms. Prior to joining the firm, David trained at another international law firm in Scotland and spent a year studying in Paris.

Simmons & Simmons

Simmons & Simmons is a leading international law firm with fully integrated teams working through offices in Europe, the Middle East and Asia, bringing experienced professionals to some of the most active growth markets today. We believe it is who we are and how we approach our work that sets us apart from other firms. We set the highest standards for the work we do, meaning you will benefit from the highest quality client service. Our focus on a small number of sectors means we are able to understand and respond to our clients' needs. Our industry sectors are: Asset Management & Investment Funds; Financial Institutions; Life Sciences; and Telecoms, Media & Technology (TMT). We also focus on the E&I market, in particular through our international projects and construction teams. We have a track record for innovation and delivering value to clients through new ways of working.

Ten Questions to Ask Before Launching a Bug Bounty Program

Serrin Turner

Latham & Watkins LLP

Alexander E. Reicher

For those outside the data security community, bug bounty programs might seem counterintuitive—and not worth the risk. Why would a company pay total strangers to "hack" into its applications, websites or devices? Why encourage the very behavior you're trying to protect against?

Bug bounty programs certainly should be approached with caution and are not for all companies. But, if thoughtfully set up and appropriately staffed and maintained, a bug bounty program can be an important component of a company's overall information security program, particularly for businesses that sell software or offer internet-facing products or services. After all, hacking forums and other black markets for information about security vulnerabilities have existed for years. Bug bounty programs are one way of competing against those illegitimate marketplaces in order to keep a company's security vulnerabilities out of the wrong hands.[1]

Further, as regulators such as the Federal Trade Commission pay increasing attention to the issue of vulnerability management, a well-designed bug bounty program can help ensure that a company has procedures in place for identifying and remediating vulnerabilities that are robust and will stand up to regulatory scrutiny. Leading technology firms have long offered monetary rewards for significant reports of security vulnerabilities from ethical hackers, pursuant to carefully crafted rules governing eligibility and authorized use. In recent years, such programs—whether self-administered or offered as a service by third-party providers—have become an increasingly standard layer of protection for companies in the tech, IT, financial services, and e-commerce sectors in particular.[2]

Below we discuss ten key questions that any company should ask before launching a bug bounty program to address security vulnerabilities in their website or app. These are of course not the *only* questions that merit consideration, but they provide a framework to begin thinking through the relevant issues.

1 Do You Need a Bug Bounty Program?

A bug bounty program is a species of what are more generally known as "vulnerability disclosure programs"—programs that solicit input on security vulnerabilities that third parties discover in a company's products or services. In theory, security researchers can test anything programmed with code—from mobile apps, to web apps, to hardware, to internet-of-things (IoT) devices—for security vulnerabilities. Having protocols and procedures in place to respond to security vulnerabilities reported by outside researchers is an important aspect of vulnerability management, as regulators have increasingly observed.[3] Indeed, the FTC has made clear that the key factors that can trigger an enforcement action related to the security of internet-connected products are a (1) well-known (2) security vulnerability (3) that causes significant harm. Thus, failure to timely attend to a credible third-party security warning, leading in turn to a security incident affecting consumers, is one of the more common scenarios that has led the FTC to pursue action under Section 5 of the FTC Act.[4]

A bug bounty program is a special type of vulnerability disclosure program that *incentivizes* third parties to report security vulnerabilities by offering them monetary rewards. Whether your company needs *a bug bounty program*—as opposed to an unpaid vulnerability disclosure program—depends on a number of factors, including the systems you already have in place to discover vulnerabilities and the resources you have to plan, launch, and maintain a bug bounty program. But for some companies, particularly those with a large "attack surface" or that are otherwise subject to a high volume of cybersecurity threats, a bug bounty program can be a cost-effective way to complement existing cybersecurity initiatives, especially compared to the cost of hiring full-time security researchers.[5] There are many reliable third-party platforms offering bug bounty programs as a service that can eliminate or reduce many of the start-up costs involved.

2 What Do You Want Your Bug Bounty Program to Address?

Assuming you have decided to launch or participate in a bug bounty program, you should consider whether you want researchers to identify vulnerabilities site-wide or on a particular set of applications, subdomains, products, or services. That decision depends on a number of factors, including whether certain parts of your website or app process particularly sensitive data (such as consumer databases or corporate IP), already have additional security in place, or are subject to special legal obligations or restrictions (such as those related to sensitive health information).[6]

You should also think about what types of security vulnerabilities you want your company's bug bounty program to address and should describe them as specifically as possible in your program's terms.[7] For example, you may want your bug bounty program to address software bugs and misconfigured systems, but not password-related vulnerabilities.[8] It may make sense to direct researchers to only some of the types of vulnerabilities your company faces—particularly if you plan to address the excluded categories of vulnerabilities through other means, such as through hired outside security consultants or your own security review and research. This incentivizes researchers to address the types of vulnerabilities with which you need assistance and, at the same time, makes clear that you will only pay bounties for reports that are in scope.[9] A list of out-of-scope issues can

further help steer researchers away from particularly unpromising or unwanted areas of research, by making explicit that they are not bounty-eligible.

3 What Guidance Do You Need to Provide Researchers on How to Test Your Website or App?

It is important to communicate to researchers not only the types of vulnerabilities you want your program to address, but also the ways you will permit them to conduct their research. In the program terms, you should clearly state what research techniques are not authorized under your program, what parts of your service are off limits, and what researchers may and may not do with data they access through their testing and hacking.[10] This will help guide researchers to solve the security problems you need solved in the way you want to solve them.

Proper guidance also serves to explain to researchers what kinds of conduct you consider "authorized" under anti-hacking laws. Broadly speaking, the Computer Fraud and Abuse Act (CFAA) prohibits accessing a computer without, or in excess of, authorization.[11] Researchers need your "authorization" to do the kind of vulnerability testing you want them to do without running afoul of the CFAA. Without clear guidance, researchers may not report the vulnerabilities they discover for fear that you (or others) will take legal action against them for their actions in testing your services.[12]

Equally important, however, is that you steer researchers away from any aspects of your services you cannot authorize them to access—such as parts of your website hosted by third-party vendors (e.g., cloud services) as to which you cannot validly authorize this kind of testing.[13] It is critical that you do not encourage researchers to hack third-party websites without authorization, since that could subject *you* to liability for contributing to or encouraging that unauthorized conduct.

4 How Are You Going to Determine How Much to Pay Researchers for Their Reports?

According to one survey, only 15% of security researchers expect a payment in return for their vulnerability reports; many mainly seek an acknowledgement when the vulnerability is disclosed, which can be important for building a researcher's reputation and credibility in the security community.[14] But assuming you have decided to incentivize researchers through monetary rewards, you will need to determine the criteria you will use to decide the amounts.

You are free to set your own criteria for determining bounty awards, but you should be aware that you are competing with other bug bounty programs for the time and attention of security researchers. Many programs use the severity of the vulnerability,[15] the impact it has on sensitive data,[16] and the quality of the researcher's report[17] as criteria for setting the award. There are public resources available that offer benchmark amounts for security reports of varying severity levels.[18] You should describe your reward criteria in your program's terms, at least at a general level, but consider adding language that clearly reserves your right to determine how much to pay for a given vulnerability—or not to pay at all—at your sole discretion. Bounty payments may be subject to taxes or prohibited in certain countries because of trade sanctions and other restrictions. You should consult legal counsel for guidance on how these issues might affect your program's bounty payments.

It is important to limit payments under a bug bounty program to persons engaged in authorized, responsible disclosure activity, which should be pre-defined in the program terms. A bug bounty program should not be used to make extortion payments to malicious actors. Earlier this year, the FTC amended a Section 5 complaint against Uber, following its public disclosure of a "bug bounty" payment of $100,000 the company had made to attackers claiming to have compromised Uber's databases, who demanded a six-figure payout. As the FTC alleged, the attackers "were fundamentally different from legitimate bug bounty recipients," in that they "did not merely identify a vulnerability and disclose it responsibly," but rather "maliciously exploited the vulnerability and acquired personal information relating to millions of consumers." The FTC complaint alleged that Uber's "bug bounty" payment was outside the ordinary course and was intended to conceal the underlying data breach from the public.[19]

5 What Needs to Be in Your Bug Bounty Program's Terms?

Your bug bounty program's terms constitute the primary document through which you communicate to researchers the goals of your program, how they may participate, and what they should (and should not) do when testing your website or app for security vulnerabilities. It is a legal document, and for that reason you should involve counsel in drafting it. But your program's terms should not be laden with legal or technical jargon. The most effective bug bounty program terms are written in plain language, since researchers likely lack formal legal training (although some will be familiar with anti-hacking laws like the CFAA) and overly technical descriptions are unnecessary and only lead to a confusing set of terms. In addition, the clearer your bug bounty program's terms, the easier it will be to deploy the same language in other contexts, such as blog posts and other marketing communications for your program.

Your program's terms should address the topics discussed above, including the scope of your program, how you authorize researchers to conduct their research on your website or app, and how you will determine bounty amounts. You should remind researchers that they are subject not only to your bug bounty program's terms, but also to any software license agreements, terms, or policies applicable to all users of your products, website or app (such as your primary terms of service and privacy notice).

You may also want to explain to researchers the consequences of failing to adhere to your program's terms, including expressly reserving the right to coordinate with law enforcement in appropriate situations. On the flip side, you should consider highlighting any benefits of complying with your program's terms. For example, you may wish to tell researchers that you will make their compliance known to a court if they are ever subject to a lawsuit by a third party with respect to actions they took within the scope of the program.[20] This kind of assurance, while not required, may encourage more researchers to participate in your program. Your program's terms may also need to address issues that are unique to the type of service you provide and, for this reason, it is important to consult with experienced legal counsel to draft terms that address these issues.

There are many model vulnerability disclosure program policies available that may serve as a useful starting point for your company's terms.[21] Alternatively, there are a variety of trusted third-party bug bounty platforms with whom you can partner, which already have preset terms.

6 Do You Have the Right Team in Place to Respond to Bug Bounty Reports in a Timely Manner?

Depending on the scale of your bug bounty program, you will need to appoint a point-person or a team of people to oversee the incoming reports, evaluate and triage the reports, and ensure that the validated security vulnerabilities identified by researchers are timely addressed by the appropriate teams.[22] A rapid response matters to the security research community: over a quarter of security researchers polled in one survey reported publicly disclosing the security vulnerability they discovered on their own because the company's response was not quick enough.[23]

Timely addressing vulnerabilities that researchers identify through your bug bounty program also matters to regulators. As noted, the FTC has taken the position that a company's failure to address a vulnerability brought to its attention by a security researcher can constitute a failure to provide reasonable and appropriate security to consumers that is actionable under Section 5 of the FTC Act.[24]

7 Do You Have the Right Platform in Place to Receive Reports?

How are researchers going to send you their reports? Will you direct researchers to an email address, a web form, or some other method? If you plan to run a bug bounty program on your own, think carefully about the security of the communication methods you ask researchers to use. Reports from researchers potentially contain the details of security vulnerabilities that could result in disastrous consequences for your company if they fell into the wrong hands. Therefore, be sure to tell researchers how to communicate their reports to you in a secure, encrypted manner.[25] Third-party bug bounty platforms often include automated and secure communications as part of the overall service.

You should also provide researchers with guidance on what information you would like their vulnerability reports to contain (and what they should *not* be sending you in those reports, such as personally identifiable information or other sensitive data).[26]

Given the risks involved in receiving and processing bug reports, outsourcing a bug bounty program to one of a number of specialty companies that host vulnerability disclosure programs is an appealing option for many organizations.[27]

8 What Is Your Launch Plan for Your Bug Bounty Program?

Just like any new product roll-out, you should prepare a launch plan for your bug bounty program. Similar to a beta release, you might roll out the program first to a smaller, private audience of familiar researchers before opening the program to the public.[28] Alternatively, you might limit the scope of the program in its initial stage, addressing only one part of your service or a more limited set of vulnerabilities. Or, you might decide to open the full program to the entire public on day one.

The right launch strategy depends on a number of factors, including, perhaps most critically, the resources you have in place to respond to and address vulnerability reports from researchers, given the importance of responding quickly as discussed above. While there is no single "right" way to launch a bug bounty program, starting with a more limited program and growing it as you develop experience dealing with incoming reports is a good default strategy.[29]

9 What Is Your Communications Plan for Rolling out Your Bug Bounty Program?

Once you have decided on your launch strategy, you will need to develop an appropriate communications plan to support that launch. The right communications channels and audience obviously depend entirely on your launch plan: it would make no sense to broadly publicize a program that you have decided to launch privately with a small group of researchers. In all cases, however, your program's policy should feature or be linked prominently on the program's landing page and in your communications plan,[30] since this includes the key language that expresses your program's intentions, scope, and limitations discussed above. You or your counsel should review all other, more informal descriptions of your program—such as any summaries of the program, frequently asked questions, or blog posts announcing the program—to ensure that these descriptions are 100% consistent with your program's terms. When in doubt, feel free to borrow language directly from your program's terms; if you have drafted your terms carefully to avoid legal or technical jargon, your policy's language should already be user-friendly and easily deployed in these other contexts.

10 How Are You Going to Deal with Reports of Security Issues That Are Beyond the Scope of Your Program or Other Unexpected Situations?

You should plan for the unexpected: researchers will inevitably report vulnerabilities beyond the scope of your program, may accidentally (or intentionally) access data that is supposed to be off limits, or may surprise you in other ways. You cannot plan for every contingency, but you should build a protocol for raising these situations with the person in charge of your bug bounty program and with counsel as soon as they are identified in the triage of incoming reports.

* * *

There are, of course, more questions beyond these to consider before launching your bug bounty program, but these legal and practical considerations should be a part of any planning discussions. With the right preparation, your bug bounty program can become a feature—not another bug—in your company's security efforts.

Endnotes

1. Kirsten E. Eichensehr, *Public-Private Cybersecurity*, 95 Tex. L. Rev. 467, 486 (2017).
2. Synack, Inc., *The Complete Guide to Crowdsourced Security Testing* (2018), https://go.synack.com/rs/738-OEX-476/images/CrowdsourcedSecurityTesting_FINAL_5-29-2018.pdf (hereafter *Synack Guide*), at 4.
3. *See* Fed. Trade Comm'n, *Start with Security* (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (hereafter *Start with Security*), at 12; *see also* Fed. Trade Comm'n, *Careful Connections: Building Security in the Internet of Things* (Jan. 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf (hereafter *FTC IoT Report*), at 8 (noting favorably reliance upon bug bounty or similar incentive programs in stimulating communication about security vulnerabilities after a product is released to the public).
4. *In re HTC America Inc.*, 155 F.T.C. 1617, 1619 (2013) (complaint) (alleging that Respondent, among other deficiencies, "failed to implement a process for receiving

and addressing security vulnerability reports from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents" in connection with the design and customization of the software on HTC mobile devices).

5. *See* Matthew Finifter, Devdatta Akhawe & David Wagner, *An Empirical Study of Vulnerability Rewards Programs*, 22ND USENIX SECURITY SYMPOSIUM 273 (2013), https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf (analyzing two well-established bug bounty programs and finding that they compared favorably to cost of hiring security researchers in-house); *see also* Rapid7 Blog, *Setting Up and Managing a Bug Bounty Program* (June 24, 2017), https://blog.rapid7.com/2017/06/24/setting-up-and-managing-a-bug-bounty-program/ (hereafter *Rapid7 Bug Bounty Guide*).
6. Computer Crime & Intellectual Property Section, Criminal Division, U.S. Department of Justice, *A Framework for a Vulnerability Disclosure Program for Online Systems* (July 2017), https://www.justice.gov/criminal-ccips/page/file/983996/download (hereafter *CCIPS Framework*), at 2.
7. Allen D. Householder, Garret Wassermann, Art Manion & Chris King, *The CERT Guide to Coordinated Vulnerability Disclosure* (Aug. 2017) (hereafter *CERT Guide*), at 42.
8. *CCIPS Framework*, *supra* note 6, at 3.
9. *CERT Guide*, *supra* note 7, at 42.
10. *CCIPS Framework*, *supra* note 6, at 6.
11. 18 U.S.C. § 1030.
12. NTIA, *Vulnerability Disclosure Attitudes and Actions* (2016), https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf (hereafter *NTIA Survey*), at 2, 6.
13. *CCIPS Framework*, *supra* note 6, at 4.
14. *NTIA Survey*, *supra* note 12, at 2, 7.
15. *See*, *e.g.*, *Policy*, DROPBOX (Jul. 9, 2018), https://hackerone.com/dropbox; *How Much Is A Bug Worth? Introducing Bounty Statistics*, HACKERONE (Dec. 13, 2016), https://www.hackerone.com/blog/bounty-statistics; *Synack Guide*, *supra* note 2, at 13. Some programs use the Common Vulnerability Scoring System (CVSS) to determine the severity of the vulnerability. *See Common Vulnerability Scoring System SIG*, FIRST.ORG, INC., https://www.first.org/cvss/.
16. *See*, *e.g.*, *Google Vulnerability Reward Program (VRP) Rules*, GOOGLE, https://www.google.com/about/appsecurity/reward-program/; *Information*, FACEBOOK (Apr. 18, 2018), https://www.facebook.com/whitehat.
17. *See*, *e.g.*, *Information*, FACEBOOK (Apr. 18, 2018), https://www.facebook.com/whitehat; *Client Bug Bounty Program*, MOZILLA, https://www.mozilla.org/en-US/security/client-bug-bounty/.
18. *See*, *e.g.*, Adam Bacchus, *Bug Bounty Field Manual*, HACKERONE, https://www.hackerone.com/resources/bug-bounty-field-manual (hereafter *HackerOne Field Manual*), at 14.
19. Revised Complaint ¶¶ 25-27, In re Uber Technologies, Inc., No. 152-3054 (F.T.C. Apr. 11, 2018), https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_complaint_0.pdf.
20. *CCIPS Framework*, *supra* note 6, at 7.
21. *See*, *e.g.*, *Policy*, DROPBOX (Jul. 9, 2018), https://hackerone.com/dropbox ("In order to encourage the adoption of bug bounty programs and promote uniform security best practices across the industry, Dropbox reserves no rights in this bug bounty policy and so you are free to copy and modify it for your own purposes."); ISO/IEC, *Information technology — Security techniques — Vulnerability disclosure (ISO/IEC 29147:2014(E))* (2014) (hereafter *ISO Vulnerability Disclosure Framework*), at 10-11, Annex B; NTIA Safety Working Group, *"Early Stage" Coordinated Vulnerability Disclosure Template, Version 1.1* (Dec. 15, 2016), https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf.
22. *CCIPS Framework*, *supra* note 6, at 5.
23. *NTIA Survey*, *supra* note 12, at 5.
24. *See* Complaint ¶¶ 17-19, *In re Fandango*, LLC, No. C-4481 (F.T.C. Aug. 13, 2014), available at https://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf (alleging that Fandango (1) lacked a defined process for receiving reports of security vulnerabilities, and (2) failed to proactively test for the vulnerability at issue); Complaint ¶¶ 20-23, In re ASUSTek Computer Inc., No. C-4587 (F.T.C. Jul. 28, 2016), available at https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf (alleging that in June 2013, a security researcher publicly disclosed that several thousand ASUS routers had a vulnerability that permitted unauthenticated access to a certain ASUS product called AiDisk, and that the security researcher reported the issue again in November 2013, and that only in January 2014 (about seven months later), did ASUS began taking steps to correct the firmware); *see also Start with Security*, *supra* note 3, at 12 (2015).
25. *ISO Vulnerability Disclosure Framework*, *supra* note 21, at 9.
26. *CCIPS Framework*, *supra* note 6, at 5.
27. *See*, *e.g.*, *CERT Guide*, *supra* note 7, at 23-24; *Rapid7 Bug Bounty Guide*, *supra* note 5.
28. *Synack Guide*, *supra* note 2, at 7.
29. *HackerOne Field Manual*, *supra* note 18, at 27-34.
30. *CCIPS Framework*, *supra* note 6, at 8.

Serrin Turner
Latham & Watkins LLP
885 Third Avenue
New York, NY 10022-4834
USA

Tel: +1 212 906 1330
Email: serrin.turner@lw.com
URL: www.lw.com

Serrin Turner is a partner at Latham & Watkins LLP, where he is a member of the firm's Cybersecurity & Data Privacy Practice, White Collar Defense & Government Investigations Practice, and Complex Commercial Litigation Practice. He counsels clients on a variety of matters relating to cybersecurity and computer hacking laws. Mr. Turner joined Latham following six years as an Assistant US Attorney for the Southern District of New York, where he served as the Office's lead cybercrime prosecutor. In that role, Mr. Turner handled a wide range of cybercrime investigations and prosecutions, including matters involving computer hacking, data breaches, black-market websites, trafficking in stolen payment card and personal identity information, and money laundering through digital currencies.

Alexander E. Reicher
Latham & Watkins LLP
505 Montgomery Street, Suite 2000
San Francisco, CA 94111-6538
USA

Tel: +1 415 646 8315
Email: alexander.reicher@lw.com
URL: www.lw.com

Alexander E. Reicher is an associate in the San Francisco office of Latham & Watkins LLP and a member of the firm's Global Antitrust & Competition Practice. He counsels clients on antitrust, data privacy, and data security law matters. Mr. Reicher rejoined Latham after serving a year as an attorney in the Federal Trade Commission's (FTC) Western Regional Office in San Francisco. At the FTC, Mr. Reicher worked on both competition and consumer protection matters.

LATHAM & WATKINS LLP

Latham & Watkins LLP delivers innovative solutions to complex legal and business challenges around the world. From a global platform, our lawyers advise clients on market-shaping transactions, high-stakes litigation and trials, and sophisticated regulatory matters. Latham is one of the world's largest providers of pro bono services, steadfastly supports initiatives designed to advance diversity within the firm and the legal profession, and is committed to exploring and promoting environmental sustainability.

Albania

Genc Boga

Eno Muja

Boga & Associates

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

The content of the following offences can be found in various articles of the "Criminal Code of the Republic of Albania", even though the latter does not provide a literal denomination of them.

Hacking (i.e. unauthorised access)

Hacking constitutes a criminal offence in the Albanian jurisdiction. Article 192/b/1 of the "Criminal Code of the Republic of Albania" provides that unauthorised access or excess of authorisation to a computer system or part of it, through violation of security measures, is punishable by a fine or imprisonment for up to three years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2017, 11 cases have been recorded by the Prosecution body, two of which have ended with the sentencing of the accused, but no further details have been given.

Denial-of-service attacks

Article 293/c/1 of the "Criminal Code of the Republic of Albania" provides that the creation of serious and unauthorised obstacles to harm the function of a computer system, through insertion, damage, deformation, change or deletion of data, is punishable with imprisonment for three to seven years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2017, four cases have been recorded by the Prosecution body, but no details have been given on the cases.

Phishing

Article 143/b of the "Criminal Code of the Republic of Albania" states that adding, modifying or deleting computer data or interfering in the functioning of a computer system, with the intention of ensuring for oneself or for third parties, through fraud, unfair economic benefits or causing a third party reduction of wealth, is punishable by imprisonment for six months to six years and a fine from 60,000 Leke to 600,000 Leke. According to the Final Report of the General Prosecutor on the state of criminality for the year 2017, 73 cases have been recorded by the Prosecution body, but no details have been given on the cases.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Article 293/b of the "Criminal Code of the Republic of Albania" provides that damage, deformation, change or unauthorised deletion of computer data is punishable by imprisonment for six months to three years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2017, 33 cases have been recorded by the Prosecution body, four of which have ended with the sentencing of the accused, but no details have been given on the cases.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Article 293/ç of the "Criminal Code of the Republic of Albania" provides that manufacturing, keeping, selling, giving for use, distribution or any other action to place at disposal any equipment, including a computer program, computer password, access code or any other similar data, created or adapted for breaching a computer system or a part of it, with the aim of committing a criminal act, as provided in articles 192/b, 293/a, 293/b and 293/c of the "Criminal Code of the Republic of Albania", is punishable by imprisonment for six months to five years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2017, one case has been recorded by the Prosecution body.

Identity theft or identity fraud (e.g. in connection with access devices)

Even though the "Criminal Code of the Republic of Albania" does not explicitly mention or provide an article dedicated to identity theft, article 186/a states that modifying, deleting, or omitting computer data, without the right to do so, in order to create false data, with the intention of presenting and using them as authentic, even though the created data is directly readable or understandable, are all punishable by imprisonment for six months to six years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2017, 16 cases have been recorded by the Prosecution body, one of which has ended with the sentencing of the accused, but no details have been given.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Article 186/a/2 of the "Criminal Code of the Republic of Albania" provides that when the aforementioned criminal act, as described in the provision of identity theft above, is done by the person responsible for safekeeping and administering the computer data in cooperation more than once, or has brought forth grave consequences for the public interest, is punishable by imprisonment for three to 10 years.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Article 293/b/2 of the "Criminal Code of the Republic of Albania" provides that damage, deformation, change or unauthorised deletion of computer data, when done in regard to military computer data,

national security, public order, civil protection, and healthcare or in any other computer data with public importance, is punishable by imprisonment for three to 10 years.

Failure by an organisation to implement cybersecurity measures

In virtue of Law No. 2/2017, "On cybersecurity", failure by an organisation to implement cybersecurity measures does not constitute a criminal offence. Article 21 of the Law "On cybersecurity" provides that failure to implement cybersecurity measures is considered an administrative violation and is punishable by a fine.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The Convention "On cyber crime", ratified in Albania on 25.04.2002 through Law No. 8888, provides, in article 22, that Member States of the Convention must determine the jurisdiction in cases when a cyber crime is committed in their territory or by a citizen of that state. Article 6/2 of the "Criminal Code of the Republic of Albania" provides that Albanian law is also applicable to Albanian citizens who commit a crime in the territory of another state, when the crime is at the same time punishable and as long as there is not any final decision by any foreign court for that crime. Also, article 7/a of the "Criminal Code of the Republic of Albania" states that the criminal law of the Republic of Albania is also applicable to foreign citizens who have committed a criminal act outside the territory of the Republic of Albania for which special laws or international agreements, of which the Republic of Albania is a part of, determine the application of the Albanian criminal legislation.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Article 48 of the "Criminal Code of the Republic of Albania" provides mitigating circumstances for any penalty. These circumstances include, but are not limited to: a) when the criminal act is driven by motives of positive moral and social value; b) when the criminal act is done under the influence of psychic shock caused by provocation or unfair actions of the victim or any other person; c) when the criminal act is done under the influence or unfair instruction of a superior; ç) when the person responsible for the criminal act shows deep repentance; d) when the person has replaced the damage caused by the criminal act or has actively helped to erase or minimise the consequences of the criminal act; dh) when the person presents him/herself before the competent bodies after committing the criminal act; and e) when the relations between the person who has committed the criminal act and the person who has suffered the consequences of the criminal act have returned to normal.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Article 74/a of the "Criminal Code of the Republic of Albania" states that distributing or offering to the public through computer systems materials that deny, minimise, or significantly approve or justify acts which constitute genocide or crimes against humanity is punishable by imprisonment for three to six years. Also, article 84/a of the "Criminal Code of the Republic of Albania" provides that serious threats to kill or seriously injure a person through computer systems because of ethnicity, nationality, race or religion are punishable by a fine or imprisonment for up to three years. Article 119/a of the "Criminal Code of the Republic of Albania" states that offering or distributing to the public through computer systems materials with racist or xenophobic content constitutes an administrative violation and is punishable by a fine or imprisonment for up to two years. Article 119/b of the "Criminal Code of the Republic of Albania" provides that a public insult involving ethnicity, nationality, race or religion through a computer system constitutes an administrative violation and is punishable by a fine or imprisonment for up to two years.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

1. The Convention "On cyber crime" ratified in Albania on 25.04.2002 with Law No. 8888.
2. Law No. 7895, dated 27.01.1995, "Criminal Code of the Republic of Albania", as amended.
3. Law No. 2/2017 "On cybersecurity".
4. Law No. 9918, dated 19.05.2008, "On electronic communications in the Republic of Albania", as amended.
5. Law No. 9887, dated 10.03.2008, "On protection of personal data", as amended.
6. Law No. 8457, dated 11.02.1999, "On classified information 'Secrets of State'".
7. Law No. 9880, dated 25.02.2008, "On electronic signatures", as amended.
8. The Decision of Council of Ministers No. 141, dated 22.02.2017, "On organising and functioning of the national authority for electronic certification and cybersecurity".

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Article 8 of the Law "On cybersecurity" specifies that operators of critical infrastructure of information are obliged to implement the requirements of safety measures, and to also document their implementation. Article 9/3 of the Law "On cybersecurity" provides that the Responsible Authority for Electronic Certification and Cybersecurity (herein the "Authority") determines, through a regulation, the content and method of documenting the safety measures. To the best of our knowledge, no such regulation exists.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Article 9 of the Law "On cybersecurity" provides a list of safety measures and divides them into two groups: organisational measures;

and technical measures. As specified above, the Authority determines, through a regulation, the content and method of documenting the safety measures. To date, no such regulation exists.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

To the best of our knowledge, no such conflict of laws issues arise.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Article 11 of the Law "On cybersecurity" provides that operators of critical infrastructure of information and operators of important infrastructure of information are obliged to report immediately to the Authority after they discover any Incidents. The Authority determines, through a specific regulation, the types and categories of Incidents regarding cybersecurity. In the case of Incidents at constitutional institutions (for example, those of security and defence), the Authority reports immediately to the directors of these institutions. In addition, article 12 provides the type of information which is kept and administered in the electronic register of the Authority: data regarding the Incident report; data on identification of the system in which the Incident happened; data on the source of the Incident; and the procedure for solving the Incident and its result. Article 14 states that the Authority shall maintain full confidentiality of the data collected during the process of solving the Incident.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Organisations are required to share information related to Incidents or potential Incidents, with contact points determined by the operators of critical infrastructure of information or the operators of important infrastructure of information. The Authority has also provided a standard form to be completed in case of Incidents.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

To the best of our knowledge and after carefully reviewing the legislation, there are no provisions as regards this situation.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The responses to questions 2.5 to 2.7 do not change regardless of the information included.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Article 8 of the Law "On cybersecurity" provides that operators of critical infrastructure of information and operators of important infrastructure of information are obliged to implement the safety measures and also document their implementation. Furthermore, the aforementioned operators are obliged to implement the requirements of the safety measures during the establishment of infrastructure.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Article 22 of the Law "On cybersecurity" states that in case of non-compliance with the requirements specified in the law, the Authority issues fines from 20,000 Leke to 800,000 Leke.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

To the best of our knowledge there are no examples of enforcement action taken in cases of non-compliance with the abovementioned requirements.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

There is not any difference as regards the variety of measures taken across different business sectors, because the Law "On cybersecurity" is applied the same regardless of the business sector.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The Law "On cybersecurity" is the only one governing with regard to cybersecurity for all organisations, private or public, in the Republic of Albania.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

The Law "On cybersecurity" does not elaborate on this point, but nevertheless this is a matter of regulation inside the company.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

To the best of our knowledge, there is no obligation to fulfil these requirements. The Authority shall draft, approve and publish the necessary regulations to complete the legislative frame for cybersecurity within 12 months of the date of the law's approval.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

The Law "On cybersecurity", even though it does not clearly mention companies, provides the obligation to report to the competent authorities. However, the "Code of Criminal Procedure of the Republic of Albania" demands disclosure when legally asked by the Prosecution, be it through an order or a court decision.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

To the best of our knowledge, companies are not subject to any other specific requirements under Applicable Laws in relation to cybersecurity.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

For a civil action to be brought in relation to any Incident, it is necessary to provide the element of damage caused by a person committing an illegal action and evidence the causality of this action. It is also necessary to identify the source or the person responsible for the Incident.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

To the best of our knowledge, there are no specific examples of cases brought in relation to Incidents.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

The Law "On cybersecurity" does not provide any specifics in this regard, but there is potential liability in tort in relation to an Incident, in virtue of the "Civil Code of the Republic of Albania", as specified above.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

To the best of our knowledge, organisations are not prohibited from taking out insurance against Incidents.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations to insurance coverage against specific types of loss, such as business interruption, etc.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

Article 9 of the Law "On cybersecurity" states that responsible bodies should take the necessary measures to manage and monitor the safety of human resources and people's access.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

To the best of our knowledge and after carefully reviewing the current Albanian legislation on the matter, there are no prohibitions in this regard.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Structures for cyber crime at the County Directory Police and General County Directory Police are responsible for investigating any crimes related to cybersecurity. In addition, the State Police has made available to the public a website (http://www.policia.al/denonco/) where every person can report in real-time any criminal act related to cyber crimes. The Authority is also responsible for investigating any reported crimes related to cybersecurity.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

To the best of our knowledge, there are no requirements under Applicable Laws for organisations to implement backdoors in their IT systems.

Genc Boga
Boga & Associates
40/3 Ibrahim Rugova Str.
1019 Tirana
Albania

Tel: +355 4 2251 050
Email: gboga@bogalaw.com
URL: www.bogalaw.com

Genc Boga is the founder and Managing Partner of Boga & Associates, which operates in both jurisdictions of Albania and Kosovo. Mr. Boga's fields of expertise include business and company law, concession law, energy law, corporate law, banking and finance, taxation, litigation, competition law, real estate, environment protection law, etc.

Mr. Boga has solid expertise as an advisor to banks, financial institutions and international investors operating in major projects in the energy, infrastructure and real estate sectors. Thanks to his experience, Boga & Associates is retained as a legal advisor on a regular basis by the most important financial institutions and foreign investors.

He regularly advises the EBRD, IFC and the World Bank on various investment projects in Albania and Kosovo.

Mr. Boga is continuously ranked as a leading lawyer in Albania by major legal directories: *Chambers Global*; *Chambers Europe*; *The Legal 500*; and *IFLR 1000*.

He is fluent in English, French and Italian.

Eno Muja
Boga & Associates
40/3 Ibrahim Rugova Str.
1019 Tirana
Albania

Tel: +355 4 2251 050
Email: emuja@bogalaw.com
URL: www.bogalaw.com

Eno Muja is an Associate at Boga & Associates.

His core practice area is litigation overarching a wide range of legal issues in Albania, mainly related to private law.

Eno represents international clients in district courts and appeal courts, in cases dealing with real estate, employment law and all sorts of other commercial/corporate disputes.

Additionally, he has also covered practice areas in IP Law and Data Protection.

Eno graduated in Law at the State University of Tirana and obtained a Master of Science degree focused on Private Law in 2014. He has been a member of the Albanian Bar Association since 2016.

Eno is fluent in English, Italian, and French.

BOGA & ASSOCIATES

LEGAL · TAX · ACCOUNTING

Boga & Associates, established in 1994, has emerged as one of the premier law firms in Albania, earning a reputation for providing the highest quality of legal, tax and accounting services to its clients. The firm also operates in Kosovo (Pristina), offering a full range of services. Until May 2007, the firm was a member firm of KPMG International and the Senior Partner/Managing Partner, Mr. Genc Boga, was also the Senior Partner/Managing Partner of KPMG Albania.

The firm's particularity is linked to the multidisciplinary services it provides to its clients, through an uncompromising commitment to excellence. Apart from the widely consolidated legal practice, the firm also offers the highest standards of expertise in tax and accounting services, with keen sensitivity to the rapid changes in the Albanian and Kosovo business environment.

The firm delivers services to leading clients in major industries, banks and financial institutions, as well as to companies engaged in insurance, construction, energy and utilities, entertainment and media, mining, oil and gas, professional services, real estate, technology, telecommunications, tourism, transport, infrastructure and consumer goods.

The firm is continuously ranked as a "top tier firm" by major directories: *Chambers Europe*; *The Legal 500*; and *IFLR 1000*.

Australia

Phillip Gibson

Nyman Gibson Miralis

Dennis Miralis

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

In New South Wales, Australia, unauthorised access to computer systems is criminalised by both state and federal legislation, namely, the *Crimes Act 1900* (NSW) ("the Crimes Act") and the Commonwealth Criminal Code ("the Code"). Most commonly, persons suspected of engaging in cybercrime are charged pursuant to the Code, given its universal application in all states and territories in Australia.

Persons suspected of unauthorised access to computer systems are charged pursuant to s. 478.1 of the Code, which provides for the offence of "Unauthorised access to, or modification of, restricted data". The offence is comprised of three elements of proof. The offence is committed if a person causes any unauthorised access to, or modification of, restricted data, the person intends to cause the access or modification and the person knows that the access or modification is unauthorised. The maximum penalty for a contravention of s. 478.1 of the Code is two years' imprisonment.

Denial-of-service attacks

Denial-of-service attacks ("DoS attacks") or Distributed Denial of Service attacks ("DDoS attacks") are criminalised by s. 477.3 of the Code, which provides for the offence of "Unauthorised impairment of electronic communication". The offence is comprised of two elements. The offence is committed if a person causes any unauthorised impairment of electronic communication to or from a computer and the person knows that the impairment is unauthorised. The maximum penalty for a contravention of s. 477.3 of the Code is 10 years' imprisonment.

Phishing

Phishing, being a form of online fraud, is criminalised by both the Crimes Act and the Code. However, enforcement of online fraud is generally left to the law enforcement agency of the state in which the victim of the fraud resides. In New South Wales, fraud is criminalised by s. 192E of the Crimes Act. The offence is comprised of three elements. The offence is committed if a person who, by any deception, dishonestly obtains property belonging to another or obtains any financial disadvantage or causes any financial disadvantage. The maximum penalty is 10 years' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

The infection of IT systems with malware is criminalised by s. 478.2 of the Code, which provides for the offence of "Unauthorised impairment of data held on a computer disk etc.". The offence is comprised of three elements. The offence is committed if a person causes any unauthorised impairment of the reliability, security or operation of data held on a computer disk, a credit card, another device used to store data by electronic means, the person intends to cause the impairment and the person knows that the impairment is unauthorised. The maximum penalty is two years' imprisonment.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Possession or use of hardware, software or other tools used to commit cybercrime is criminalised by s. 478.3 of the Code, which provides for the offence of Possession or control of data with intent to commit a computer offence. The offence is comprised of two elements. The offence is committed if a person has possession or control of data and the person has that possession or control with the intention that the data be used, by the person or another person, in committing an offence against Division 477 of the Code or facilitating the commission of such an offence. The maximum penalty for a contravention of s. 478.3 of the Code is three years' imprisonment.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity crime, and in particular identity fraud offences, are criminalised by Division 372 of the Code. Particular acts that are criminalised include dealing in identification information, dealing in identification information that involves use of a carriage service, possession of identification information and possession of equipment used to make identification information. The offence of "Dealing in identification information that involves use of a carriage service" is most relevant to cybercrime. It is criminalised by 372.1A of the Code and is comprised of four elements. The offence is committed if a person deals in identification information, the person does so using a carriage service, the person intends that any person will use the identification information to pretend to be, or to pass the user off as, another person (whether living, dead, real or fictitious) for the purpose of committing an offence or facilitating the commission of an offence, and the offence is an indictable offence against the law of the Commonwealth, an indictable offence against a law of a State or Territory, or a foreign indictable offence. The maximum penalty is five years' imprisonment.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft is criminalised by s. 478.1 of the Code. As the offence is committed if a person modifies restricted data, and

modification is defined in the Code as the alteration or removal of the data held in a computer, or an addition of the data held in a computer, the unauthorised copying of data from a computer would contravene the offence provision.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Part 10.6 of the Code creates offences related to telecommunication services. They include offences relating to dishonesty with respect to carriage services and interference with telecommunications.

Failure by an organisation to implement cybersecurity measures

See the discussion below in relation to corporate governance.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Extended geographical jurisdiction applies to offences under Part 10.7 of the Code (Divisions 477 and 478).

A person will not commit offences under that Part unless: the conduct constituting the alleged offence occurs wholly or partly in Australia, or wholly or partly on-board an Australian aircraft or an Australian ship; or the conduct constituting the alleged offences occurs wholly outside Australia and a result of the conduct occurs wholly or partly in Australia, or wholly or partly on-board an Australian aircraft or an Australian ship; or the conduct constituting the alleged offence occurs wholly outside Australia and at the time of the alleged offence, the person is an Australian citizen or at the time of the alleged offence, the person is a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory; or all of the following conditions are satisfied: the alleged offence is an ancillary offence; the conduct constituting the alleged offence occurs wholly outside Australia; and the conduct constituting the primary offence to which the ancillary offence relates, or a result of that conduct, occurs, or is intended by the person to occur, wholly or partly in Australia or wholly or partly on-board an Australian aircraft or an Australian ship.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

In New South Wales, the penalties for criminal offences are prescribed by the *Crimes Sentencing Procedure Act 1999* (NSW). The *Crimes Act 1914* (Cth) prescribes the penalties applicable to breaches of federal legislation, such as the Code. Matters that generally will mitigate a penalty include the timing of any guilty plea, the offender's character, the offender's prior record, assistance provided by the offender to the authorities, and the offender's prospect of rehabilitation and likelihood of reoffending. Notification would be a matter that could be taken into account by a sentencing court as a factor of mitigation.

A number of the offences particularised above cannot be "attempted"; they must actually be committed. For example, a person cannot attempt to commit the offence of "Unauthorised access, modification or impairment with intent to commit a serious offence".

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

A number of criminal offences may arise in relation to cybersecurity or the occurrence of an Incident, although they are best understood as tangential or ancillary to cybersecurity or the occurrence of an Incident. For example, there have been prosecutions for offences such as blackmail where an offender has used material obtained as a result of a breach of confidence to blackmail the owner by threatening to release that material online.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The following laws in New South Wales relate to cybersecurity: the *Privacy Act* (Cth) ("Privacy Act"); the *Crimes Act 1914* (Cth); the *Security of Critical Infrastructure Act 2018* (Cth); the *Criminal Code 1995* (Cth); and the *Telecommunications (Interception and Access) Act 1979* (Cth).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The *Security of Critical Infrastructure Act 2018* (Cth), which commenced on 11 July 2018, seeks to manage national security risks of sabotage, espionage and coercion posed by foreign entities. The Act was implemented as a response to technological changes that have increased cyber connectivity to critical infrastructure. The Australian Government considers "the responsibility for ensuring the continuity of operations and the provision of essential services to the Australian economy and community" as being shared "between owners and operators of critical infrastructure, state and territory governments, and the Australian Government". The Act applies to approximately 165 specific assets in the electricity, gas, water and ports sectors.

The Act establishes a Register of Critical Infrastructure Assets, empowers the Secretary of the Department of Home Affairs with an information-gathering power (whereby certain information can be requested of direct interest holders, responsible entities and operators of critical infrastructure assets) and a Minister directs power that allows the Minister to issue a direction to an owner or operator of critical infrastructure assets to mitigate national security risks.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

See generally the answer to question 4.3 below in respect of the NDB Scheme.

The Australian Securities and Investments Commission ("ASIC") provides guidance to Australia's integrated corporate markets, financial services and consumer regulator, and provides guidance to organisations through its "cyber reliance good practices". The good

practices recommend, *inter alia*, periodic review of cyber strategy by a board of directors, using cyber resilience as a management tool, for corporate governance to be responsive (i.e. keeping cybersecurity policies and procedures up to date), collaboration and information sharing, third-party risk management and implementing continuous monitoring systems.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

See the answer to question 4.3 below.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

See the answer to question 4.3 below.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Subject to the restrictions in the Applicable Laws (such as the Privacy Act), organisations are permitted to voluntarily share information related to an Incident or potential Incidents with a regulatory or other authority and other private sector or trade associations.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

See the answer to question 4.3 below.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

See the answer to question 4.3 below.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Office of the Australian Information Commissioner ("the OAIC") is an independent statutory agency within the Attorney-General's Department. The OAIC has three functions, namely, privacy functions conferred by the Privacy Act, freedom of information functions such as reviewing the decisions made by agencies and ministers pursuant to the *Freedom of Information Act 1982* (Cth), and government information policy functions conferred by the *Australian Information Commissioner Act 2010* (Cth).

In relation to its privacy functions, the OAIC has the power to commence investigations, conduct privacy performance assessments, request an entity to develop an enforceable code, direct an agency to give the OAIC a privacy impact assessment about a proposed activity or function and recognise external dispute-resolution schemes to handle privacy-related complaints.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

See the answer to question 4.3 below.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

To date, there have been no published examples of enforcement action taken in cases of non-compliance with the Notifiable Data Breaches ("NDB") Scheme.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practice varies across different business sectors in New South Wales. The NDB Scheme, for example, only requires not-for-profit businesses with an annual turnover of more than AUD $3 million to report data breaches.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Part IIIA of the Privacy Act specifically regulates the handling of personal information about individuals' activities in relation to consumer credit, including the types of personal information that credit providers can disclose. All credit reporting bodies (defined in ss 6 and 6P as a business that involves collecting, holding, using or disclosing personal information about individuals for the purposes of providing an entity with information about the creditworthiness of an individual) are subject to Part III.

Part 13 of the Telecommunications Act regulates carriers and carriage service providers in their use and disclosure of personal information. Part 5-1A of the Telecommunications (Interception and Access) Act

1979 (Cth) requires providers of telecommunications services in Australia to collect and retain specific types of data for a minimum period of two years and must comply with the Privacy Act in relation to that data.

See generally the answer to question 4.3 below for more information. The NDB Scheme in Part IIIC of the Privacy Act requires telecommunications and financial services sectors to take steps to secure personal information. These sectors must notify individuals whose personal information is involved in a data breach that is likely to result in serious harm and must also notify the OAIC.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

A failure by a company to prevent, mitigate, manage or respond to an Incident may result in breaches of provisions of the *Corporations Act 2001* (Cth). The *Corporations Act 2001* (Cth) imposes duties on directors to exercise powers and duties with the care and diligence that a reasonable person would. A director who ignores the real possibility of an Incident may be liable for failing to exercise duties with care and diligence.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Presently, the Applicable Laws do not require companies to designate a CISO, establish a written Incident response plan or policy, conduct periodic cyber risk assessments and perform penetration tests or vulnerability assessments.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

In February 2018 the Privacy Amendment (Notifiable Data Breaches) Act 2017 amended the Privacy Act to require Australian Privacy Principles ("APP") entities to, as soon as practicable, provide notice to the OAIC and affected individuals of an "eligible data breach", where there are reasonable grounds to believe that an "eligible data breach" has occurred. This process is called the Notifiable Data Breaches Scheme.

Eligible data breaches arise when: there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds; this unauthorised disclosure of personal information, or loss of personal information is likely to result in serious harm to one or more individuals; and the entity has not been able to prevent the likely risk of serious harm with remedial action.

The OAIC expects APP entities to conduct a quick assessment of a suspected data breach to determine whether it is likely to result in serious harm.

The notification to the OAIC and to the affected individual must include the identity and contact details of the organisation, a description of the data breach, the kinds of information concerned and recommendations about the steps individuals should take in response to the data breach.

A failure to comply with the notification obligations can result in the imposition of substantial civil penalties. A serious or repeated interference with privacy attracts a fine of 2,000 penalty units, currently AUD $420,000.00. The maximum penalty that a court can order for a body corporate is five times the amount listed in the civil penalty provision, currently a maximum of AUD $2.1 million.

The Privacy Act also confers a number of additional enforcement powers on the OAIC, including accepting an enforceable undertaking, bringing proceedings to enforce an enforceable undertaking, making a determination, bringing proceedings to enforce a determination, a report to the responsible Minister and seeking an injunction.

Under the Privacy Act, an APP entity is defined as an "agency" or "organisation". "Agency" includes a Minister, a Department, and most government bodies; and an "organisation" means an individual, a body corporate, a partnership, any other unincorporated association or a trust that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

The Australian Privacy Principles contained in schedule 1 of the Privacy Act provide for the manner in which APP entities must handle and use personal information. There are 13 privacy principles, covering: open and transparent management of personal information; anonymity and pseudonymity; collection of solicited personal information; dealing with unsolicited personal information; notification of the collection of personal information; the use or disclosure of personal information; direct marketing; cross-border disclosure of personal information; adoption, use or disclosure of government-related identifiers; quality of personal information; security of personal information; access to personal information; and the correction of personal information. The APPs are not prescriptive, and an APP entity must consider how the principles apply to its own situation.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Australian common law does not recognise a general right of privacy. The equitable cause of action for breach of confidence may provide a remedy for invasions of privacy. Traditionally, the elements are that information must be confidential, information must have been imparted in circumstances importing an obligation of confidence, and there must be an unauthorised use of that information. The current doctrine of breach of confidence does not currently entertain cases of wrongful intrusion, as opposed to cases of wrongful disclosure of confidential information.

The Privacy Act regulates the way Commonwealth agencies handle personal information. A person may obtain an injunction in the Federal Circuit Court against a Commonwealth agency that engages in, or proposes to engage in, conduct that is in breach of the Privacy

Act. An action cannot be brought against an individual acting in their own capacity. A person may apply to the Court for an order that an entity pay compensation for loss or damage suffered by the person if a civil penalty has been made against the entity, or the entity is found guilty of an offence under the Privacy Act.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

No relevant civil proceedings have been brought in relation to an Incident. Given the evolution of the doctrine of breach of confidence, it is likely such cases will be forthcoming.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

The High Court in *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 sanctioned the recognition of a tort of invasion of privacy. Judge Hampel in the case of *Doe v ABC* (2007) VCC 281 imposed liability in tort for the invasion of the plaintiff's privacy. Such reasoning may apply to an action in relation to an Incident.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Organisations are permitted to take out insurance against Incidents in Australia. This includes breaches of the Privacy Act.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limits specifically targeted at losses associated with Incidents. Numerous entities offer insurance for data breach, business interruption, email forgery, ransomware attacks, costs of rebuilding an IT system, theft of crypto-currencies, and legal fees associated with the investigation of Incidents. Coverage is governed generally by the *Insurance Act 1973* (Cth), the *Insurance Contracts Act 1984* (Cth), the *Corporations Act 2001* (Cth) and the common law.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The *Workplace Surveillance Act 2005* (NSW) restricts the use of both overt and covert forms of surveillance of an employee. Surveillance can include computer surveillance. Significant penalties are imposed for breaches of the Act, including imprisonment.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

Whistle-blowers are recognised and protected by the *Corporations Act 2001* (Cth). There are five criteria that must be met when a whistle-blower makes a disclosure in order to be protected by the Act. Firstly, the whistle-blower must be a current office, a current employee or a current contractor (or the employee of a contractor). Secondly, the disclosure must be made to the company's auditor or a member of the company's audit team, a director, secretary or senior manager of the company, a person authorised by the company to receive whistle-blower disclosure or ASIC. Thirdly, the whistle-blower must provide their name to the person or authority to whom the disclosure is made. Fourthly, the whistle-blower must have reasonable grounds to suspect that the information being disclosed on the company or company officer may have breached the *Corporations Act 2001* (Cth) or the *Australian Securities and Investments Commission Act 2001* (Cth). Fifthly, the disclosure must be made in good faith, in that the disclosure must be honest and genuine, and motivated by wanting to disclose misconduct.

The information disclosed by whistle-blowers is protected by ASIC, the whistle-blower is protected by the *Corporations Act 2001* (Cth) from civil or criminal litigation, and the Act also makes it a criminal offence to victimise a whistle-blower.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

A number of well-established legal investigatory powers are deployed by law enforcement authorities when investigating an Incident. These powers can include the issuing of search warrants, the seizure of IT equipment for forensic analysis, decryption (whether at encrypted or decrypted data points) and the compulsory examination of suspects, in certain circumstances.

The *Assistance and Access Bill 2018* (Cth), presently up for parliamentary debate, is seeking to expand the investigative powers of law enforcement. For example, the Bill seeks to modernise and strengthen search warrants to "account for the growing complexity of communications devices and the evidential value of data".

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Presently, there are no requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities. The Australian government has expressed that it remains "committed to the security of communications services and devices and the privacy of Australians".

Section 3LA of the *Crimes Act 1914* (Cth) provides law enforcement authorities a mechanism by which a person must provide information or assistance that is reasonable and necessary to allow a constable to access data held in, or accessible from, a computer or data storage device that is on warrant premises or that has been moved to a place for examination under subsection 3K(2) of the *Crimes Act 1914* (Cth),

copy data held in, or accessible from, a computer, or storage device and convert into documentary form or another form intelligible to a constable data held in, or accessible from, a computer, or data storage device, or data held in a data storage device to which the data was copied, or data held in a data storage device removed from warrant premises under subsection 3L(1A) of the *Crimes Act 1914* (Cth).

Phillip Gibson
Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney
New South Wales
Australia

Tel: *+61 2 9264 8884*
Email: *pg@ngm.com.au*
URL: *www.ngm.com.au*

Phillip Gibson is one of Australia's leading criminal defence lawyers with more than 30 years of experience in all areas of criminal law. Phillip manages and advises on the most complex criminal cases.

Phillip has vast experience in transnational cases across multiple jurisdictions often involving: assets forfeiture; money laundering and proceeds of crime; cybercrime; extradition; mutual assistance; white-collar crime; royal commissions; bribery and corruption; Interpol notices; international and national security law; and matters related to the Independent Commission Against Corruption and the Crime Commission.

Dennis Miralis
Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney
New South Wales
Australia

Tel: *+61 2 9264 8884*
Email: *dm@ngm.com.au*
URL: *www.ngm.com.au*

Dennis Miralis is a leading Australian defence lawyer who acts and advises in complex domestic and international criminal law matters in the following areas: white-collar and corporate crime; money laundering; serious fraud; cybercrime; international asset forfeiture; international proceeds of crime law; bribery and corruption law; transnational crime law; extradition law; mutual assistance in criminal law matters; anti-terrorism law; national security law; criminal intelligence law; and encryption law.

He appears in all courts throughout Australia and regularly travels outside Australia for complex international and transnational criminal law matters.

NYMAN GIBSON MIRALIS
Criminal Defence Lawyers and Advisors est. 1966

Nyman Gibson Miralis are experts in assisting companies and individuals who are the subject of cybercrime investigations.

The investigation and prosecution of cybercrime is becoming increasingly international. Individuals and businesses may therefore become the subject of parallel criminal investigations and prosecutions raising complex jurisdictional and procedural issues. By its very nature, cybercrime is borderless, and therefore the exposure to penalties outside the jurisdiction where an individual or business is physically located is often a real possibility.

Our criminal lawyers have expertise in dealing with complex national and international cybercrime investigations and advising individuals and businesses of defence strategies that take into account the global nature of cybercrime.

Our expertise includes dealing with law enforcement requests for information from foreign jurisdictions, challenging potential extradition proceedings, as well as advising and appearing in cases where assets have been restrained and confiscated worldwide.

Brazil

Siqueira Castro – Advogados

Daniel Pitanga Bastos De Souza

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Hacking constitutes a criminal offence in Brazil under Law No. 12.737/2012. This Law modified Provision 154-A of the Brazilian Criminal Code to provide that the invasion of a third party's computing device, whether or not it is connected to a computer network, through undue violation of a security mechanism and with the purpose of obtaining, adulterating or destroying data is a crime in Brazil. The maximum penalty for such an offence is one year of imprisonment and fine, or two years of imprisonment and a fine if the hacker obtains the victim's private electronic communications contents, commercial or industrial secrets, or sensitive information. The two years of imprisonment and a fine also apply if the hacker controls the invaded device remotely. The aforementioned penalties may be increased where there are aggravating circumstances.

Denial-of-service attacks

Denial-of-service attacks can be punished under the Brazilian Criminal Code. According to Provision 266, the interruption or disturbance of telegraph, radiotelegraph or telephone services as well as telematics services or public utility information services shall be punished with imprisonment and a fine. The maximum penalty is three years of imprisonment, and this penalty may be doubled if the offence occurs during a public calamity.

Phishing

There is no specific provision regulating phishing in Brazil.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Infection of IT systems with malware is a criminal offence in Brazil. According to Provision 154-A of the Brazilian Criminal Code (modified by Law No. 12.737/2012), the installation of vulnerabilities in a third party's computing device, whether or not it is connected to a computer network, to obtain an illicit advantage shall be punished with up to one year of imprisonment and a fine. The penalty may be increased where there are aggravating circumstances.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

There is no specific provision regulating possession or use of hardware, software or other tools used to commit cybercrime in Brazil. However, the production, offering, distribution, selling or sending of a computer program or device to allow the invasion of a third party's computing device, whether or not it is connected to a computer network, through undue violation of a security mechanism and with the purpose of obtaining, adulterating or destroying data constitutes a crime punishable with up to one year of imprisonment and a fine.

Identity theft or identity fraud (e.g. in connection with access devices)

There is no specific provision regulating identity theft or identity fraud in connection with access devices in Brazil. Notwithstanding, identity theft or identity fraud, by any means, constitute the crime of false identity, punishable with up to two years of imprisonment or a fine. Further, other criminal provisions may apply in a specific case, such as ideological falsity.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

See the answer in respect of "Hacking" and "Infection of IT systems with malware" above. Further, breach of confidence by a current or former employee is classified as unfair competition under Law No. 9279/96 (Industrial Property Law), punishable with up to one year of imprisonment or a fine.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Unfair competition provisions stated in the Industrial Property Law may apply in some circumstances. Unfair competition is a criminal offence in Brazil punishable with up to one year of imprisonment or a fine.

Failure by an organisation to implement cybersecurity measures

Failure by an organisation to implement cybersecurity measures is not a criminal offence in Brazil.

1.2 Do any of the above-mentioned offences have extraterritorial application?

There is no specific provision regulating extraterritorial application of cybersecurity crimes in Brazil. However, as a rule, Brazilian criminal provisions may apply outside its territory in some circumstances provided by law.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

There are possibilities for penalty mitigation in specific circumstances (e.g. cooperation with investigations).

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

At first, any criminal offence perpetrated in a cybernetic context may be punished in the same way as it would if committed outside of such context. In this sense, a very common offence is the crime of extortion in the context of a ransomware cyberattack.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Besides the Applicable Laws mentioned above, which refer to criminal offences, there are important provisions related to civil rights in the Brazilian Internet Law (*Marco Civil da Internet*) and its regulatory Decree No. 8.771/2015. Further, the Brazilian Constitution, Consumer Code, and Industrial Property Law have scattered provision relating to themes that may be connected to cybersecurity. Moreover, the Brazilian President signed the first ever Brazilian Data Protection Law on 14 August 2018, which will come into force by February 2020. Concerning this Law, organisations will be required to implement technical measures to safeguard personal data. Furthermore, the Central Bank of Brazil has recently issued Resolution No. 4.658/2018, which will fully come into force on 31 December 2021, concerning the adoption of measures in the field of cybersecurity.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Yes. Generally, cybersecurity requirements are provided by regulatory agencies. For instance, financial services providers, regulated by the Central Bank of Brazil, have specific rules related to cybersecurity. As mentioned above, the Central Bank of Brazil has recently issued Resolution No. 4.658/2018, which regulates the adoption of measures in the field of cybersecurity.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the Brazilian Data Protection Law, which will be in force by February 2020, organisations will be required to take security, technical and administrative measures to safeguard personal data. Further, an organisation that processes personal data and suffers an Incident shall provide, within reasonable time, information concerning such Incident to the Authority and to the data subject.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Yes. Adoption of measures to monitor, detect, prevent or mitigate Incidents may conflict with Applicable Laws and Tribunal precedents (e.g. the right of privacy of the employee in the workplace).

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes. According to the Brazilian Data Protection Law, which will be in force by February 2020, controllers must inform the Data Protection Authority of any occurrence of a security Incident that may create risk or relevant damage to the data subjects. The communication shall be done in a reasonable period (to be determined by the Data Protection Authority) and shall contain a description of the nature of the affected personal data, information regarding data subjects, indication of the adopted technical and security measures to protect the data, the risks related to the Incident, and the measures that were or will be taken to reverse or mitigate the effects of the damage. Further, in case the communication was not immediate, the controller must provide reasons for the delay.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

There is no legal basis to share information related to Incidents or potential Incidents with third parties, as it is not provided by the Data Protection Law.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes. According to the Brazilian Data Protection Law, which will be in force by February 2020, controllers must inform affected

individuals of any occurrence of a security Incident that may create risk or cause relevant damage to them. The communication shall be done in a reasonable period (to be determined by the Data Protection Authority) and shall contain a description of the nature of the affected personal data, information regarding the data subjects, an indication of the adopted technical and security measures to protect the data, the risks related to the Incident, and the measures that were or will be taken to reverse or mitigate the effects of the damage. Further, in case the communication was not immediate, the controller must provide reasons for the delay.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No. See the answer provided in response to question 2.6.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Brazilian Data Protection Law had referred to the Data Protection Authority as the Regulator; however, the Brazilian President vetoed the chapter dedicated to this Authority because of a lack of formality as requested by the Brazilian Constitution. In view of that, the Data Protection Authority was not incorporated into the Data Protection Law, but the President is committed to proposing a specific law to create the Authority. It is expected that this Authority will have powers to regulate data protection, to monitor companies' and individuals' compliance with the Data Protection Law and to impose sanctions regarding breaches of the Law.

In addition, other regulators may supervise compliance with sector regulations and standards (e.g. the Central Bank of Brazil may supervise the compliance of financial institutions with its Resolution No. 4.658/2018).

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The Brazilian Data Protection Law (due by February 2020) provides penalties for infringements, including: a warning, indicating the deadline for the adoption of corrective measures; a single fine of up to 2% of the company's, group's or conglomerate's revenues in Brazil in its last fiscal year, excluding taxes, up to R$ 50,000,000.00 per infraction; a daily fine; publicisation of the infraction after it has been duly verified and its occurrence is confirmed; blockage of the personal data to which the infraction relates, until regularisation thereof; and elimination of the personal data to which the infringement relates.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

As the Brazilian Data Protection Law will not come into force until February 2020, there are, as of yet, no examples.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes. Banks and financial companies are usually more committed to information security because of the risks involved in their business (e.g. identity theft and identity fraud are widely perpetrated in Brazil). Notwithstanding, we foresee an increase in measures to prevent, detect, mitigate and respond to Incidents in other sectors in the coming years because of the enactment of the Brazilian Data Protection Law.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes. The Brazilian Central Bank has recently issued a regulation on cybersecurity policy and the contracting of data processing and storage and cloud computing to be observed by financial institutions and other institutions regulated by the Central Bank (Resolution No. 4.658/2018).

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

A breach of directors' duties would arise if the failure happens due to a director's action that is not compliant with the law or with the company's bylaws.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The Brazilian Data Protection Law determines that controllers shall appoint a Data Protection Officer, who will be in charge of communications with the Data Protection Authority and data subjects, as well as of controllers' compliance. The Data Protection Law does not oblige the controller to create an Incident response plan, conduct periodic cyber risk assessments or perform penetration tests or vulnerability assessments, but the adoption of such measures may mitigate possible penalties. Moreover, the Data Protection Authority may regulate those matters in the future.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

The Brazilian Data Protection Law provides that controllers must inform the Data Protection Authority and data subjects of any

occurrence of a security Incident that may create risk or relevant damage to the data subject.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

The Brazilian Data Protection Law provides that processing agents (controllers and processors) shall adopt security, technical and administrative measures to protect personal data from unauthorised accesses and accidental or unlawful situations of loss, alteration, destruction, communication or any improper or unlawful processing of data. Such measures shall be complied with by processing agents from the conception through to the execution of the product or service.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The civil actions that may be brought depend on the nature of the Incident, but in general, Incidents involving breach of privacy, data theft, ransomware, and breach of the Brazilian Data Protection Law are dealt with by means of a tort lawsuit. Given the distribution of liability defined in the Brazilian Data Protection Law, there is also a possibility for the data processing company to be sued.

With regards to the elements that must be met in such action, it is notable that the defendant must be identified. In this sense, if the person/company responsible for the Incident is not known, the claimant must file a previous lawsuit against the internet service provider through which the person responsible for the Incident has operated. In this previous lawsuit, the claimant would need to request that the internet provider inform the IP of the party responsible for the Incident. However, in some circumstances, it may not be possible to identify the person responsible for the Incident. This is one of the main legal difficulties in dealing with cyberattacks in Brazil.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

A well-known ticket sales company was responsible for an Incident in which personal data of registered clients was exposed upon access of the company's website. The Incident was caused by a security failure in the company's website and gave rise to a huge number of lawsuits.

Additionally, the Consumer Protection Authority issued a notice to the company, requesting information regarding the Incident and the measures taken to prevent such event from happening again. In this case, although there was no Data Protection Law in force in Brazil, the Consumer Protection Authority may request the adoption of measures to companies in any circumstance that involves consumers' rights. Also, the Consumer Protection Authority may apply a fine based on the Consumer Code.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes. Brazilian law allows individuals and companies to file a lawsuit claiming damages in any situation, including in relation to an Incident.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no such regulatory limitations.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There are no such specific requirements.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no such Applicable Laws.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Upon an Incident investigation, the police authority, the administrative authority or the Public Prosecutor may require, as a preventive measure, any application service provider to keep access to applications logs, including for a period greater than that provided in the Brazilian Internet Law. In all circumstances, the disclosure to the authorities and prosecutors must be preceded by a court order.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no such requirements.

Daniel Pitanga Bastos De Souza
Siqueira Castro – Advogados
Praça Pio X, 15, 3º andar
Rio de Janeiro – RJ
Brazil

Tel: *+55 21 2514 7496*
Email: *dpitanga@siqueiracastro.com.br*
URL: *www.siqueiracastro.com.br*

Daniel Pitanga Bastos de Souza graduated from the Catholic University of Salvador in 2006. He gained a postgraduate degree in intellectual property law from the Catholic University of Rio de Janeiro and specialised in entertainment law at the State University of Rio de Janeiro. He also holds an LL.M. in information technology and telecommunications law from the University of Southampton. He is a member of the Brazilian Bar Association, Rio de Janeiro section and secretary-general of the Industrial Property and Piracy Committee at the Brazilian Bar Association, Rio de Janeiro section. He is the Co-Chair of the Interactive Entertainment and Media Committee at the International Technology Law Association (ITechLaw).

SIQUEIRA CASTRO
ADVOGADOS

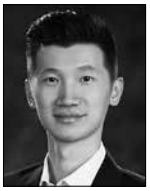
Considered one of the most traditional and prestigious law firms in Brazil, with 83 partners and 823 associates, Siqueira Castro – Advogados is a pioneering full-service business law firm with offices throughout the country. Over its 70-year history, our firm has consistently met the great range of our clients' legal needs with a full spectrum of services and excellent results in all areas of business law. Moreover, our clients have come to trust that our structure will constantly benefit from solid and regular investments in resources and personnel.

Today, in addition to our headquarters in São Paulo, the firm is present in 18 state capitals of Brazil, namely: Rio de Janeiro, Brasília, Aracaju, Belém, Belo Horizonte, Curitiba, Fortaleza, João Pessoa, Maceió, Manaus, Natal, Porto Alegre, Porto Velho, Recife, Salvador, São Luís, Teresina and Vitória. This unrivalled geographical reach enables convenient access to all relevant economic centres of the country. In the international arena, we have taken steps to make the firm one of the most active Brazilian players abroad, with the incorporation of our Lisbon (Portugal) and Luanda (Angola) branches. We also maintain strategic alliances with reputable firms in Brazil, Latin America, North America, Asia, Africa and Europe, many as a consequence of our participation in ADVOC, the international network of independent law firms – www.advoc.com – of which Siqueira Castro – Advogados is the only Brazilian member.

What sets Siqueira Castro – Advogados apart is more than just the performance of its highly qualified professionals, many of whom have both worked and studied abroad. It is the personalised services that the firm devotes to projects, deals and businesses that call for understanding of many specialties. We leverage the force inherent in our highly organised structure to bring speed, safety, flexibility, efficiency and cost savings to every task in our charge.

China

Susan Ning



King & Wood Mallesons

Han Wu

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Under the *Criminal Law of the People's Republic of China* ("Criminal Law"), cybercrimes are mainly provided in the section: "Crimes of Disturbing Public Order". Articles 285, 286, and 287 are the three major articles that directly relate to cybercrimes. Moreover, Article 253(1) indirectly relates to cybersecurity and applies to cases involving Internet-related personal information infringement acts. The punishments for violating Articles 285, 286, and 287 include imprisonment, detention, and fines. For example, the offender may be sentenced to up to seven years' imprisonment for illegally obtaining data from a computer information system in serious cases. Entities may be convicted for violating Articles 285, 286, and 287, as unit crime has been provided for in all three articles.

It is worth noting that Articles 286 and 287 set up the principle that if someone uses computers (for example, through hacking, phishing or other Internet-related illegal action) to commit other crimes, i.e. crimes that traditionally had no relationship with the Internet, such as financial fraud, theft, embezzlement, misappropriation of public funds and theft of state secrets, the offender shall be convicted of the crime for which the penalty is heavier.

Hacking (i.e. unauthorised access)

Pursuant to Article 285 of the *Criminal Law*, activities which involve invading a computer information system in the areas of State affairs, national defence or advanced science and technology constitute the "crime of invading a computer information system". The offender shall be sentenced to a fixed-term imprisonment of not more than three years or detention. For activities of invading a computer information system other than those in the above areas, it may constitute a "crime of obtaining data from a computer information system and controlling a computer information system" and the offender shall be sentenced to a fixed-term imprisonment of not more than three years or detention, or imprisonment for three to seven years in serious cases. If an entity commits those crimes, such entities shall be fined, and the persons who are directly in charge and the other persons who are directly liable for the offences shall be punished accordingly.

For example, in the criminal case of "Wang's illegal obtainment of computer information system data and controlling a computer system", according to the final decision made by Fuyang Intermediate People's Court in Anhui Province in May 2018, the defendant was sentenced to three years in prison but suspended for five years and fined 8,000 yuan for illegally obtaining more than 9,000 pieces of personal information by using self-learning hacking technology.

Denial-of-service attacks

Pursuant to Article 286 of the *Criminal Law*, denial-of-service attacks could constitute the "crime of sabotaging computer information system" and more than five years' imprisonment may be given in serious cases.

Phishing

Phishing is usually performed to steal or otherwise acquire personal information of citizens, which is considered as the "crime of infringing a citizen's personal information" provided in Article 253(1) and up to seven years' imprisonment may be sentenced in serious cases.

For example, in the criminal case of "Zhang Dawei's infringement upon a citizen's personal information", the defendant established a phishing website to counterfeit the official website of Apple iCloud. In this way, the defendant obtained a victim's Apple ID and password and then sold them for profit. The court decided that the defendant committed the "crime of infringing a citizen's personal information" and imposed seven months' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

For intentional creation or dissemination of a computer virus or other destructive programs, including, but not limited to, ransomware, spyware, worms, trojans and viruses, which affect the normal operation of a computer information system, if serious consequences are caused, such activities constitute the "crime of sabotaging a computer information system" under Article 286 of the *Criminal Law*. The offender may be sentenced to five years' imprisonment in serious cases.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

If someone possesses or uses hardware, software or other tools to commit cybercrime prescribed in the *Criminal Law*, depending on the crime committed, the offender may be convicted in accordance with the corresponding article in the *Criminal Law*, such as the "crime of invading a computer information system".

There is also an offence, i.e. "illegal use of information networks", which involves activities that take advantage of an information network to establish websites and communication groups for criminal activities, such as defrauding, teaching criminal methods, producing or selling prohibited items and controlled substances. If

the criminal activity also constitutes another offence, the offender shall be convicted of the crime which imposes a heavier penalty.

Identity theft or identity fraud (e.g. in connection with access devices)

Under the *Criminal Law*, for identity theft, if the offender obtains identities by stealing or otherwise illegally acquires the personal information of citizens, such activity may be convicted as the "crime of infringing a citizen's personal information" pursuant to Article 253(1). If someone uses the stolen identity of others as its own proof of identity, such behaviour may constitute the "crime of identity theft" under Article 281 of the *Criminal Law*; in case such person uses the stolen identity to commit fraud or other criminal activities, he/she should be convicted of the crime the penalty of which is higher.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

If a current or former employee breaches confidentiality obligations and causes infringement of personal information, trade secrets, state secrets, etc., the offender will be convicted pursuant to Article 287 and punished in accordance with the relevant provisions of the *Criminal Law*, such as the "crime of infringing trade secrets".

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

If someone, in violation of laws and regulations, deletes, amends, adds or disturbs functions of a computer information system and causes the computer information system's inability to work normally or conducts operations of deletion, amendment or addition towards the data or application programs which are stored, disposed of or transmitted in a computer information system, and serious consequences are caused, such activities constitute the "crime of sabotaging computer information system" under Article 286 of the *Criminal Law*. The offender shall be sentenced to a fixed-term imprisonment of more than five years if serious consequences are incurred.

Failure by an organisation to implement cybersecurity measures

Pursuant to Article 286(1) of the *Criminal Law*, if an organisation is a network service provider, and does not perform its duties of safety management, provided by laws and administrative regulations, on its information network, and refuses to correct its conduct after the regulatory authorities order it to rectify the non-performance, the organisation shall be fined, and the persons who are directly in charge and the other persons who are directly liable for the offences may be sentenced to a fixed-term imprisonment of no more than three years, under any of the following circumstances:

(1) resulting in the dissemination of a large amount of illegal information;

(2) causing the disclosure of user information, resulting in serious consequences;

(3) causing the damage or loss of criminal evidence which results in serious consequences; or

(4) other serious circumstances.

1.2 Do any of the above-mentioned offences have extraterritorial application?

All of the above-mentioned offences have extraterritorial application. First, if the criminal act or its consequence takes place within the territory of China, the crime shall be deemed to have been committed within the territory of China. Second, the *Criminal Law* is applicable to citizens of China who commit crimes prescribed in the *Criminal Law* outside the territory of China; however, if the maximum penalty of such crime prescribed in the *Criminal Law* is a fixed-term imprisonment of not more than three years, the offender could be exempted from punishment. Third, if a foreigner commits a crime outside the territory of China against the State or against Chinese citizens, the offender may be convicted pursuant to the *Criminal Law* if the *Criminal Law* prescribes a minimum punishment of fixed-term imprisonment of not less than three years; but, the *Criminal Law* shall not apply if it is not punishable according to the law of the place where it was committed.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

For the above-mentioned offences, there are no specific mitigation conditions prescribed in these articles. However, the mitigation conditions prescribed in the *Criminal Law* for all crimes are applicable. For example, if an offender voluntarily gives oneself up to the police and confesses his crimes or exposes others' crimes that can be verified, the offender would be given a mitigated punishment.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Article 287(2) of the *Criminal Law* provides for the "crime of assisting information network criminal activity", which regulates activities of providing Internet access, server hosting, network storage, communication transmission and other technical support while being aware that others use such information networks to commit criminal offences (e.g. activities that lead to cybersecurity Incidents or terrorism activities).

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The Cybersecurity Law of the People's Republic of China ("**Cybersecurity Law**"), which came into force on 1 June 2017, is a law covering various aspects of network security and has laid the foundation for a comprehensive cybersecurity regulatory regime in China. So far, a series of specific measures aimed at facilitating the implementation of the *Cybersecurity Law* have already been enacted, such as the *Measures on the Security Review of Network Products and Services (for Trial Implementation)* and the *National Emergency Response Plan for Cybersecurity Incidents*. In addition, the *Regulation on Graded Protection of Network Security* is also seeking opinions. Meanwhile, the draft regulations and guidelines on the protection of critical information infrastructure ("**CII**") and security assessment of outbound data transfers have been finished and the relevant authorities are now seeking opinions, including the draft *Regulations on the Security Protection of Critical Information Infrastructure*, the draft *Measures for the Security Assessment of*

Personal Information and Important Data to be Transmitted Abroad, and the draft *Guidelines for the Security Assessment of Cross-Border Data Transfer*.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The *Cybersecurity Law* includes provisions on the security protection of CII. The draft *Regulations on the Security Protection of Critical Information Infrastructure* further specify the requirements on the security protection of critical information infrastructure, including CII operators' obligations relating to the setting up, suspension of operation and occurrence of security Incidents of CII, daily security maintenance, security monitoring and assessment, local data storage and security assessment of outbound data transfers, security of network products and services procured, etc.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. The *Cybersecurity Law*, the *Regulations on the Security Protection of Computer Information System*, the *Emergency Response Plan for Cybersecurity Incidents*, and other relevant laws and regulations have provided for network operators' legal duties when facing cybersecurity Incidents, which in general could be categorised into the following:

(1) regular preventive work: network operators must adopt regular measures to prevent cybersecurity Incidents, including adopting technical measures to prevent cybersecurity violations such as computer viruses, cyberattacks and network intrusions, adopting technical measures to monitor and record the network operation status and cybersecurity events, maintaining cyber-related logs for no less than six months, etc.;

(2) emergency measures for security Incidents: network operators must develop an emergency plan for cybersecurity Incidents in order to promptly respond to security risks, to take remedial actions immediately, to notify affected data subjects, and to report the case to the competent authorities as required; and

(3) after-action review: to keep communication with and assist the authorities in finishing their investigation and review after an Incident, such as providing a summary of the cause, nature, and influence of the security Incident and improvement measures.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Conflict of laws issues may arise, as although China's cybersecurity laws and regulations in general apply to network operators within the territory of China, any activities outside China that may threaten the cybersecurity of China could also be governed by Chinese laws.

For example, in terms of import/export controls of encryption software and hardware, pursuant to the *Regulation on the Administration of Commercial Cipher Codes* of China, import of encryption products and equipment with encryption technology or export of commercial encryption products shall be approved by the national encryption administrations. Any sale of foreign encryption products by an entity or individual is prohibited.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes.

(a) The reporting obligation will be triggered by the occurrence of an Incident threatening network security.

(b) Pursuant to the *Cybersecurity Law* and relevant regulations, network operators shall at least timely notify the local government, industry regulator and local cyberspace administrations. Pursuant to the *Regulations of the People's Republic of China on the Security Protection of Computer Information System*, any case arising from computer information systems shall be reported to the public security authority within 24 hours. Moreover, if there is a possibility of information leakage related to national security, the national security authorities shall also be informed.

(c) At least the following contents are required to be reported: information of the notification party; description of the network security Incident; detailed information about the Incident; nature of the Incident; affected properties (if any); personal information being affected/breached (if any); preliminary containment measures that have been taken; and preliminary assessment on the severity of the Incident.

(d) If the publication of Incident-related information will jeopardise national security or public interest, then such publication shall be prohibited.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Pursuant to the *Cybersecurity Law*, the authorities support the cooperation among network operators in the collection, analysis and notification of cybersecurity information and the emergency response, in order to improve their capability for cybersecurity protection. But the releasing of cybersecurity information, such as system bugs, computer viruses, network attacks and intrusions, to the public shall be carried out in compliance with the applicable regulations.

In China, users, suppliers and research institutions are encouraged to report any potential system vulnerabilities identified to the China National Vulnerability Database, an official database operated by the National Network Emergency Response Coordination Center

of China, so as to gather, verify and warn against any security vulnerabilities and to establish an effective and coordinated emergency response mechanism among all operators.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Under the *Cybersecurity Law*, in case of disclosure, damage or loss, or possible disclosure, damage or loss, of user information, the network operator is obligated to take immediate remedies and notify the affected users promptly. Currently, relevant laws and regulations do not provide specific requirements about the nature and scope of information to be reported; according to the *Information Security Techniques – Personal Information Security Specification*, recommended standards formulated by the National Standardization Committee, operators shall at least inform data subjects of the general description of the Incident and its impact, any remedial measures taken or to be taken, suggestions for individual data subjects to mitigate risks, contact information of the person responsible for dealing with the Incident, etc.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

When reporting an Incident to the regulatory authorities, network operators are required to provide any information relating to the Incident as required by the authorities, even if such information involves sensitive business information or personal identifiable information, so as to effectively cooperate with the authorities in investigating and dealing with the Incident.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Any regulators identified under question 2.5 above to which network operators are required to report an Incident shall have the authority to enforce the requirements identified under questions 2.3 to 2.7. Specifically, the enforcement authorities include the Cyberspace Administration of China ("**CAC**"), the Ministry of Industry and Information Technology, the Ministry of Public Security, the State Secrecy Bureau, the State Encryption Administration and industry regulators, etc.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Pursuant to the *Cybersecurity Law*, in case of non-compliance, network operators may be given a warning, ordered to take rectification measures, and/or imposed fines by the relevant authorities.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

One of the first enforcement actions taken since the implementation of the *Cybersecurity Law* relates to the failure to maintain web logs. The cybersecurity team of the public security bureau of Chongqing Municipality gave warnings to a company providing a data centre service for failure to keep a web log, as required by the *Cybersecurity Law*, and ordered it to rectify the non-compliance.

In late July 2017, the CAC, the Ministry of Industry and Information Technology, the Ministry of Public Security, and the National Standardization Committee jointly initiated an inspection on the "privacy policy" of network operators to identify any non-compliance with the rules of personal information protection.

Also, early in May 2017, before the implementation of the *Cybersecurity Law*, 15 data companies were questioned by the CAC, challenging the legality of data collection.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Although industries or sectors such as telecoms, credit reporting, banking and finance, and insurance have some specific requirements with respect to the collection and protection of information, the prevention of information leakage, and the emergency response to Incidents, these requirements are, in general, in line with those under the *Cybersecurity Law* without deviations.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes. For example, the *Provisional Rules on Management of the Individual Credit Information Database* is promulgated by the People's Bank of China to ensure the secure and legitimate use of personal credit information. In addition, pursuant to the *Provisions on Protecting the Personal Information of Telecommunications and Internet Users*, telecommunication business operators or Internet information service providers shall record information such as the staff members who perform operations on the personal information of users, the time and place of such operations, and the matters involved, to prevent user information from being divulged, damaged, tampered with or lost.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Under the *Cybersecurity Law*, if a company, as a network operator, fails to fulfil the obligation of security protection to ensure that the

network is free from interference, disruption or unauthorised access, and to prevent network data from being disclosed, stolen or tampered with, fails to satisfy the mandatory requirements set forth in the applicable national standards, or fails to develop an emergency plan for cybersecurity Incidents, a fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the responsible person directly in charge.

Moreover, as mentioned in question 1.1 above, pursuant to Article 286(1), if a network service provider fails to perform its duties of security protection on the information network as required by laws and administrative regulations, and refuses to correct their conduct after the regulatory authorities order them to rectify the non-performance, the network operator shall be fined, and the persons who are directly in charge and the other persons who are directly liable for the offences may be sentenced.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Under the *Cybersecurity Law*, all network operators are required to designate a person in charge of cybersecurity, such as a CISO, to establish an emergency plan for cybersecurity Incidents, and to take technical measures to monitor and record network operation and cybersecurity events.

In addition, pursuant to Article 38 of the *Cybersecurity Law*, CII operators are required to conduct, by themselves or entrusting a service provider, an examination and assessment of their cybersecurity and the potential risks at least once a year, and submit the examination and assessment results, as well as improvement measures, to the competent authorities in charge of the security of the CII. That is to say, periodic cyber risk assessments and vulnerability assessments are mandatory for CII operators.

There is no clear requirement to include third-party vendors in the scope of the risk assessment. However, critical network equipment and special-purpose cybersecurity products provided by third-party vendors should satisfy the compulsory requirements set forth in the national standards and shall not be sold or supplied until such equipment or product successfully passes security certification or security tests by a qualified organisation.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Please refer to the answers to questions 2.5, 2.6 and 2.7 above.

In addition, listed companies may have the duty to disclose cybersecurity risks or Incidents to the China Securities Regulatory Commission or disclose such information in their annual reports, depending on whether such information is deemed as significant and required to be disclosed.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

In general, network operators' obligations in relation to cybersecurity under relevant laws and regulations include maintaining the security of the network operation, and protecting the security of network information. The *Cybersecurity Law* has established the relevant mechanism for the above purpose, such as regulations in relation to personal information protection, CII protection, cross-border data transmission, emergency response for Incidents, and security review of network products and services. Under each of these mechanisms, network operators are subject to specific obligations.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

From the perspective of individuals, if an Incident results in unauthorised access to or disclosure of personal information collected and kept by the network operator, the individuals affected could bring a lawsuit against such network operator for breach of security protection obligations or for disclosing personal information by negligence on the basis of tort pursuant to the *General Provisions of the Civil Law of the People's Republic of China* and the *Tort Law of the People's Republic of China*.

Further, as confirmed by the decision on the *Sina/Maimai* case by the Beijing Intellectual Property Court, user data/information is an important operating resource of and confers competitive advantages to network operators. If a network operator "steals" data from its competitor by accessing the data of such competitor without authorisation, the aggrieved party could sue the infringing party for unfair competition on the basis of the *Anti-unfair Competition Law of the People's Republic of China*.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Qunar, a major online ticket-booking platform in China, and China Eastern Airlines were sued by one of its users for tort before the First Intermediate People's Court of Beijing in March 2017, as the user's personal information, including name and telephone number, was disclosed by Qunar and China Eastern Airlines to a third party who sent phishing messages to such user, claiming that the flight booked was cancelled. The court ordered Qunar and China Eastern Airlines to apologise to the plaintiff.

As mentioned in question 5.1 above, in the *Sina/Maimai* case, Maimai illegally accessed and collected user information from Sina without authorisation, Sina brought a lawsuit against Maimai for unfair competition, and the court upheld the claims made by Sina and ordered Maimai to stop its illegal activities, apologise in public, and compensate Sina.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Please refer to the answer to question 5.1.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations may take out insurance against Incidents, provided that such insurance categories are within the permitted scope of

insurance regulations and have been approved by or filed with the China Insurance Regulatory Commission (CIRC). Currently, in China, there are already several insurance agents providing insurance related to Incidents such as data leakage, hacking, etc.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

So far, we are not aware of any regulation that sets out limitations specifically on insurance against Incidents. Normally, the coverage of loss will be decided through private negotiation between the insurer and the applicant, as long as such coverage does not violate mandatory regulations in China.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

Article 21 of the *Cybersecurity Law* has set out several general obligations for network operators in terms of the issue of employees, including formulating internal security management systems and operation instructions, and determining a person in charge of cybersecurity so that his responsibility will be clearly defined.

Apart from that, pursuant to Article 34 of the *Cybersecurity Law*, CII operators shall establish a dedicated security management body, designate a person in charge, and review the security backgrounds of the said person and those in key positions. Furthermore, CII operators are also obliged to provide the relevant employees with regular cybersecurity education, technical training and skill assessment.

It is understood that specific requirements on the monitoring of employees or reporting by employees may be stipulated in the internal rules or policies of network operators for the purpose of security protection.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

From the perspective of commercial practice, as companies impose confidentiality obligations on their employees (say, in the employment contract or separate confidentiality agreement or internal company rules and policies), an employee's reporting of the vulnerability of his company's network system to a third party would probably lead to a failure to fulfil such obligations.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In accordance with the *Cybersecurity Law* and other relevant regulations, generally there are several enforcement agencies that are entitled to have investigatory power regarding an Incident, such as:

(1) CAC, which is responsible for the overall planning and coordination of cybersecurity work and the relevant supervision and administration; and

(2) the authority in charge of telecommunication, the public security authority and other relevant authorities of the State Council, which will take charge of protecting, supervising and administrating cybersecurity pursuant to the present regulations in China.

The specific investigatory power of the above enforcement agencies can be found in a number of laws and regulations. For example, as stated in Article 54 of the *Cybersecurity Law*, the relevant departments of the government at provincial level and above are entitled to take the following measures in case of an increasing risk of an Incident:

(1) require authorities, organs and personnel concerned to promptly collect and report necessary information;

(2) organise authorities, organs and professionals concerned to analyse and evaluate cybersecurity risks; and

(3) give warnings to the public about the cybersecurity risks and release prevention and mitigation measures.

Pursuant to Article 19 of the *Anti-Terrorism Law of the People's Republic of China* ("**Anti-Terrorism Law**"), where a risk of terrorism may arise in an Incident, the CAC, competent telecommunications department, public security department, as well as the national security department shall engage the following actions in accordance with their respective duties:

(1) order the relevant entities to stop transmission and delete the information involving terrorism and extremism; and

(2) shut down the relevant sites, and cease the related services.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

First, the *Cybersecurity Law* has made it clear that network operators shall provide technical support for the public security department and the national security department specifically on two matters: 1) safeguarding national security; and 2) investigation of crimes. Second, the *Anti-Terrorism Law* explicitly states that telecommunications operators and Internet service providers shall facilitate the relevant departments in terrorism cases, such as providing technical interfaces and decryption services. Moreover, for entities and individuals which engage in international network connections, public security departments may also ask them to provide information, materials and digital files on security protection matters when investigating crimes committed through computer networks connected with international networks.

Susan Ning
King & Wood Mallesons
40th Floor, Office Tower A
Beijing Fortune Plaza
7 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
China

Tel: *+86 10 5878 5010*
Email: *susan.ning@cn.kwm.com*
URL: *www.kwm.com*

Susan is a Senior Partner and the head of the compliance team in KWM. She is one of the pioneers engaged in the cybersecurity and data compliance practice, with publications in a number of journals such as the *Journal of Cyber Affairs*. Her publications include *New Trends of the US Personal Data Protection – Key Points of the New FCC Rules*, *Big Data: Success Comes Down to Solid Compliance*, *Does Your Data Need a "VISA" to Travel Abroad?*, and *A Brief Analysis on the Impact of Data on Competition in the Big Data Era*, etc.

Susan's practice areas cover self-assessment of network security, responding to network security checks initiated by authorities, data compliance training, due diligence of data transactions or exchanges, compliance of cross-border data transmissions, etc. Susan has assisted companies in sectors such as IT, transportation, online payment, consumer goods, finance and Internet of Vehicles in dealing with network security and data compliance issues.

Han Wu
King & Wood Mallesons
40th Floor, Office Tower A
Beijing Fortune Plaza
7 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
China

Tel: *+86 10 5878 5749*
Email: *wuhan@cn.kwm.com*
URL: *www.kwm.com*

Han is a Partner in the compliance team in KWM. He practises in the areas of cybersecurity, data compliance and antitrust. He is good at providing cybersecurity and data compliance advice to multinational companies' branches in China from the perspective of data compliance in China. At the same time, Han can also establish network security and data compliance systems for Chinese enterprises going abroad in line with the requirements of the European Union (GDPR), the United States and other cross-jurisdictions.

In the area of cybersecurity and data compliance, Han provides legal services including: assisting clients in establishing a cybersecurity compliance system; assisting clients in self-investigation on cybersecurity and data protection; assisting clients in conducting internal training on cybersecurity and data compliance; assisting clients in due diligence in data transactions; assisting clients in designing a plan for cross-border data transfers; and assisting clients in network security investigations and cybersecurity incidents, etc.

KING&WOOD MALLESONS
金杜律师事务所

King & Wood Mallesons is an international law firm headquartered in Asia that advises Chinese and overseas clients on a full range of domestic and cross-border transactions, providing comprehensive legal services. Around the world, the firm has over 2,000 lawyers with an extensive global network of 27 international offices spanning Singapore, Japan, the US, Australia, the UK, Germany, Spain, Italy and other key cities in Europe as well as presences in the Middle East. With a large legal talent pool equipped with local in-depth and legal practice, it provides legal services in multiple languages. King & Wood Mallesons, with its strong foundation and ever-progressive practice capacity, has been a leader in the industry. It has received more than 300 international and regional awards from internationally authoritative legal rating agencies and business and legal media, including *Acritas*, *Financial Times*, *ALB*, *Who's Who Legal*, *Chambers Asia-Pacific* Awards, *Euromoney*, *LEGALBAND*, *Legal Business*, *The Lawyer*, etc.

Denmark

Niels Dahl-Nielsen

Daniel Kiil

Synch

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Hacking, in the narrow sense of gaining unauthorised access to another's information or to programs intended to be used in an information system, is a criminal offence punishable by a fine or imprisonment of up to one year and six months according to the Danish Criminal Code ("DCC"). In the presence of aggravating circumstances, or if the offence is of a more systematic or organised character, the punishment is imprisonment of up to six years.

In one case, a person received a penalty equal to a fine of DKK 2,000 for gaining unauthorised access to another person's social media account.

Denial-of-service attacks

Denial-of-service attacks are punishable by a fine or imprisonment of up to one year according to the DCC, which criminalises preventing another from using or having access to, including the use of, its information systems.

In the presence of aggravating circumstances or if the offence is of a more systematic or organised character, the punishment is imprisonment of up to two years.

Phishing

Phishing is, as identity theft, not criminalised as such, but usually forms part of another criminal offence such as data fraud.

In some circumstances, sending an email with false information may be punishable as falsification of documents according to the DCC. In that case, the punishment is a fine, imprisonment of up to two years or, in the presence of aggravating circumstances or in case of a high number of offences, imprisonment of up to six years according to the DCC.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Destructive attacks on IT systems are considered vandalism according to the DCC and are punishable by a fine or imprisonment of up to one year and six months. In case of repeat offenders or vandalism of a more systematic or organised character, the punishment is imprisonment of up to six years.

Destructive attacks on systems that are vital to society are punishable by a fine or imprisonment of up to six years according to the DCC.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

The development or possession of malicious software is not criminalised in general. However, when accompanied with preparatory acts such as the establishment of communication channels where the source is not identifiable, the potential perpetrator may be punished for an attempt to spread the malware, which is punishable in the same manner as if the malware was spread successfully.

Manufacturing, acquisition, etc. of information that can be used to identify means of payment or generated payment card numbers is punishable by a fine or imprisonment of up to one year and six months according to the DCC. In the presence of aggravating circumstances, the punishment is imprisonment of up to six years.

According to the DCC, unauthorised acquisition or communication of access codes, or other means of access to information systems reserved for paying users, is a criminal offence and punishable by a fine or imprisonment of up to one year and six months. In the presence of aggravating circumstances, the punishment is imprisonment of up to six years.

Possession for commercial purposes, sale, etc., of tools intended to bypass DRM protection is a criminal offence and punishable by a fine according to the Danish Copyright Act.

Possession, manufacturing, etc., of and advertising for decoders or other decoding equipment for the purpose of giving unauthorised access to the contents of an encrypted radio or TV programme is punishable with a fine according to the Danish Radio and Television Act. Intentional offences in the presence of aggravating circumstances are punishable by imprisonment of up to one year and six months.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity theft is not criminalised as such but usually leads to or forms part of another criminal offence such as falsification of documents, hacking, theft, fraud, or data fraud.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

The Danish Act on Trade Secrets criminalises unlawful acquisition, use, and disclosure of trade secrets and, *inter alia*, eases the requirements for the use of provisional and precautionary measures. A trade secret is defined as information that is not generally known, has commercial value because it is a secret, and has been subject to reasonable measures to keep it secret.

Employees of telecommunications companies are subject to specific legislation regarding information about the usage of the company's service under the Danish Telecommunications Act.

Data fraud is punishable by imprisonment of up to one year and six months, or up to eight years if the offence is of a particularly aggravated nature according to the DCC. Data fraud includes, in particular, unauthorised wire transfers and the use of false or stolen credit card details.

Unauthorised reproduction or making available to the public of copyright protected works is punishable by a fine, or imprisonment of up to one year and six months if the offence is committed intentionally and in the presence of aggravating circumstances according to the Danish Copyright Act. Intellectual property infringements of a particularly aggravated nature are punishable by imprisonment of up to six years according to the DCC.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Interception of email and other electronic messages by cutting it off from the intended recipient or familiarising one with its contents is punishable by a fine, imprisonment of up to one year and six months, or imprisonment of up to six years in the presence of aggravating circumstances according to the DCC.

Opening an email that has been wrongly addressed to someone is not criminalised. However, forwarding such a message may, depending on its contents, be punishable as unauthorised communication of messages concerning another's private matters according to the DCC.

Commercial sale or a greater dissemination of codes or other means of access to an information system not available to the public is punishable by a fine or imprisonment of up to one year and six months according to the DCC. In the presence of aggravating circumstances, the punishment is imprisonment of up to six years according to the DCC.

According to the DCC, unjustified use of information resulting from another person's hacking, interception of messages, or sale or dissemination of codes or other means of access to an information system not available to the public is punishable in the same manner as the original offence.

Failure by an organisation to implement cybersecurity measures

Under the GDPR, a data controller or processor's failure to implement appropriate security measures is subject to an administrative fine.

The failure of the board of directors of a limited liability company to ensure an adequate level of security for the company is punishable by a fine and may result in civil liability as further described under question 4.1.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The DCC applies to criminal offences committed on foreign territory when the offence is committed by a Dane or a person living in Denmark and the act is also criminalised in the foreign country (double criminality).

In relation to offences that depend on or are influenced by an intended or occurred consequence of the offence, the offence is considered as having occurred where the perpetrator intended for the consequence to materialise. As such, the Danish criminal jurisdiction covers offences where the perpetrator was not on Danish territory when committing the criminal offence if his actions had or were intended to have a consequence on Danish territory, as is often the case concerning cybercrime.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The DCC states certain general circumstances that shall be considered when determining criminal sanctions, e.g., whether the perpetrator has denounced himself and pled guilty to the offence. Further, subject to a specific assessment of the circumstances, there is a general possibility of remission or discharge.

Under the GDPR, when deciding whether to impose an administrative fine and deciding on the amount of the fine, there are several mitigating factors to be considered, such as how the supervisory authority became aware of the infringement and the degree of cooperation with the supervisory authority in order to remedy the infringement.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

The duty of confidentiality of persons operating within the public administration, according to the Danish Public Administration Act, as well as lawyers, doctors, and pastors, entails an obligation to implement adequate security measures to protect confidential information.

Destructive attacks of considerable proportions on IT systems and destructive attacks on systems that are vital to society are punishable as terrorism according to the DCC, when the act can cause serious damage to a country or an international organisation and the offence is committed in a manner that may threaten human life or cause considerable economic losses. Further, the perpetrator must have committed the offence with the intention of seriously intimidating a population, forcing the hand of public authorities or an international organisation, or destabilising or destroying the fundamental structures of a country or an international organisation. The punishment is imprisonment up to a life sentence.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Danish law does not provide a consolidated approach to cybersecurity. The following acts and orders relate directly or indirectly to cybersecurity.

Company law

- The Danish Companies Act.

Criminal law

- The Danish Criminal Code.

Critical infrastructure

- The Danish Act on Network and Information Security of Domain Name Systems and Certain Digital Services.

- The Danish Act on Requirements of Security of Network and Information Systems within the Health Sector.
- The Danish Act on Security of Network and Information Systems for Operators of Essential Internet Exchange Points etc.
- The Danish Act on Security of Network and Information Systems in the Transport Sector.

Data protection

- The General Data Protection Regulation (the GDPR).
- The Danish Data Protection Act.

Health sector

- The Danish Order on Health Preparedness Planning.
- The Danish Order on Health Records.

Intellectual property

- The Danish Copyright Act.

Financial services sector

- The Danish Financial Business Act.
- The Danish Act on Payment Services.
- The Danish Order on Management and Control of Banks etc.
- The Danish Order on Outsourcing.

Telecommunications sector

- The Danish Radio and Television Act.
- The Danish Telecommunications Act.

Other sector-specific requirements to emergency preparedness and response

- The Danish Order on Preparedness for the Natural Gas Sector.
- The Danish Order on Preparedness for the Electricity Sector.
- The Danish Order on Preparedness Relating to Offshore Oil and Gas Operations.
- The Danish Order on Preparedness Relating to Marine Pollution from Oil and Gas Installations etc.
- The Danish Order on Railway Undertakings and Railway Infrastructure Managers.
- The Danish Order on Risk-Based Municipal Emergency Services.

Other

- The Constitutional Act of the Kingdom of Denmark.
- The Danish Act on Television Surveillance.
- The Danish Act on the Centre for Cyber Security.
- The Danish Act on Trade Secrets.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The Network and Information Systems Directive is implemented into Danish law with several sector-specific acts (listed under question 2.1 under critical infrastructure). The implementing legislation does not exceed the requirements of the directive.

Operators of essential services are, according to the relevant sector-specific legislation, required to implement an appropriate security level to control the risk to security in the network and information systems used for their activities. An operator of an essential service is generally defined as i) a unit that delivers a service that is essential for the maintenance of critical societal functions, ii) where the delivery of the service depends on networks and information systems, and iii) an Incident would have a highly disruptive effect on the delivery of the service.

Providers of digital services are subject to certain requirements according to the Danish Act on Network and Information Security of Domain Name Systems and Certain Digital Services. Digital services are generally online marketplaces, online search engines, and cloud computing-services that are not considered essential services. Providers of digital services are also required to implement an appropriate security level.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Certain companies are required to maintain adequate levels of cybersecurity, mainly by means of policies, as further described under questions 4.1–4.4.

Insofar as information that qualifies as personal data according to the GDPR is involved, data controllers and processors are required to implement an adequate level of security in relation to the risks that are presented by the processing. Further, where a type of processing is likely to result in a high risk to individuals, the data controller shall carry out an assessment of the impact of the envisaged processing operations.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Currently, no issues regarding conflict of laws have been identified, although different Acts may regulate similar areas.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

According to the GDPR, the data controller shall notify the supervisory authority of a personal data breach without undue delay after becoming aware of it. A data processor shall notify the data controller of a breach without undue delay.

Operators of essential services are required to report Incidents with an impact on the continuity of the services they deliver. The recipient of the report depends on the sector of the operator. For instance, according to the Danish Act on Net and Information Security for Domain Name Systems and Certain Digital Services, Incidents must be reported to the Danish Business Authority and the Danish Centre for Cyber Security. Such a report must namely contain information as to the number of affected users, the duration of the Incident,

and the geographical spread in relation to the area affected by the Incident. The relevant regulator can publish information about specific Incidents when necessary to prevent or manage an Incident in progress.

Similarly, providers of digital services are required to report Incidents with a substantial impact on the services they deliver to the Danish Business Authority and the Danish Centre for Cyber Security.

Providers of financial services are required to report certain Incidents to the relevant authorities, primarily the Financial Supervisory Authority, the Danish Business Authority and the Danish Centre for Cyber Security.

The Danish Business Authority has oversight of the main sections of the Danish Telecommunication Act but, depending on the type of Incident, other authorities may be involved, especially the Danish Centre for Cyber Security.

The Danish Act on Payment Services puts obligations on providers of payment services to report Incidents to the authorities to the users of the payment services if there is a risk that their transactions may be affected.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Authorities and companies can voluntarily share information related to Incidents with the Danish Centre for Cyber Security. Such voluntary notifications are exempt from the rules regarding public access to documents and allow the Danish Centre for Cyber Security to assist authorities and companies in case of an Incident.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

According to the GDPR, data controllers are required to notify data subjects without undue delay of personal data breaches that are likely to result in a high degree of risk to the rights and freedoms of the data subjects.

The Danish Act on Payment Services puts obligations on providers of payment services to report Incidents to the users of the payment services if there is a risk that their transactions may be affected.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, but insofar as the Incident relates to information that qualifies as personal data under the GDPR, the requirements of the GDPR must be respected when processing the data.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Danish Data Protection Agency is responsible for enforcing the requirements under the GDPR.

The regulator responsible for enforcing the requirements for operators of essential and digital services depends on the sector of the operator in question.

The Danish Business Authority has oversight of the main sections of the Danish Telecommunication Act.

The regulators responsible for enforcing the requirements under the Danish Act on Payment Services and for providers of financial services depends on the nature of the breach, but are primarily the Financial Supervisory Authority, the Danish Business Authority and the Danish Centre for Cyber Security.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Failure to comply with the requirements under the GDPR is subject to an administrative fine.

The failure of an essential service to comply with the requirements for such a service is punishable by a fine.

The failure to comply with the requirements under the Danish Telecommunications Act is punishable by a fine.

The failure to comply with the requirements under the Danish Act on Payment Services is punishable by a fine.

The failure to comply with requirements related to providers of financial services is subject to a fine and may be subject to imprisonment.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

There have been no notable examples of enforcement in relation to non-compliance with regulatory cybersecurity requirements thus far.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, the market practice varies across business sectors due to extensive sector-specific regulation. However, there are no common deviations from any strict legal requirements.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes, companies within the financial services sector are, *inter alia*, required to adopt a cybersecurity policy, prepare a contingency plan, and comply with an extensive set of requirements when outsourcing key activity areas.

Regarding the telecommunications sector, providers of public electronic communications networks or services are primarily subject to legal requirements under the Danish Telecommunications Act. Such providers are, *inter alia*, obliged to register themselves with the police and comply with certain rules regarding equipment, information security and emergency situations.

Further, as described under question 2.5, providers of essential services and digital services are required to report Incidents as per the above.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

According to the Danish Companies Act, in limited liability companies that have a board of directors, the board must ensure that adequate risk management and internal control procedures are established. This entails an obligation to maintain an overview of cybersecurity risks and to ensure an adequate level of cybersecurity. If such measures are found to be inadequate, an Incident may amount to a breach of the directors' duties.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Certain companies, especially in the financial sector and ones responsible for critical infrastructure (NIS Directive), are required to maintain security policies, especially related to IT security. Further, the GDPR requires technical and organisational measures to be in place.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

As per the above, certain companies are required to maintain security policies. Under certain circumstances, such policies, etc., must be disclosed to the relevant authorities.

Further, the obligations of the board of directors may include an obligation to take cybersecurity risks into account in the company's annual report.

Additionally, listed companies may be required to disclose information (regardless of whether it derives from a cybersecurity breach or not) that may affect the price of the company shares.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, besides sector-specific requirements, companies are not subject to any other specific requirements in relation to cybersecurity.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

A person or an organisation that has suffered damages as a result of another organisation's action or omission, namely by failing to comply with regulatory requirements, can claim compensation for the damages suffered. The injured party will normally have to prove that he has suffered damages, that there is a basis of liability, and that there is a causal link between the damages suffered and the action or omission giving rise to his claim.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

There have been no notable civil cases in relation to Incidents.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes, there is a potential liability in tort in relation to an Incident, but this would normally be subsidiary to other damages in Danish law.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, cyber risk insurances are permitted and gaining in popularity.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No. However, it is unclear whether it is possible to insure yourself against regulatory fines or not.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The rights of employers to monitor their employees are generally regulated by labour law regulations. Such monitoring must be reasonably justified on the grounds of the operations of the employer.

There are no general requirements regarding the reporting of cyber risks, etc., by employees to their employer. Due to the duty of loyalty arising from the employment contract, however, an employee may have to report Incidents to the employer.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no applicable laws that generally prohibit or limit the reporting of cyber risks, etc., by an employee.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The law enforcement authorities have various common powers of investigation, depending on the nature of the given case as well as which authority is investigating it.

The Danish Data Protection Agency is authorised to carry out planned and *ad hoc* investigations of authorities, companies and other data controllers and data processors. In connection with such investigations, the Danish Data Protection Agency can, *inter alia*, order any information it requires for the performance of its tasks to be provided, and obtain access to any premises of the data controller or processor.

The Centre for Cyber Security can, *inter alia*, in a number of circumstances, process package and traffic data from networks of affiliated authorities and organisations without a court order.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Providers of certain electronic communications services are obligated to make it possible for law enforcement authorities to gain insight into or listen in on communications.

Acknowledgment

We would like to thank legal intern Kristoffer Rosenquist Kirk for his valuable contribution to this chapter.

Niels Dahl-Nielsen

Synch
Strandvejen 58
1. Sal, 2900 Hellerup
Denmark

Tel: +45 7027 8899
Fax: +45 7027 8898
Email: niels.dahl-nielsen@synchlaw.dk
URL: www.synchlaw.se/da

Niels Dahl-Nielsen is a co-founder of Synch in Copenhagen. Niels heads Synch's practice within data protection and cybersecurity and has long experience within those same areas. Niels Dahl-Nielsen mainly represents companies in the IT industry within various segments – in particular, software development and software consultancy companies in all matters related to data protection and cybersecurity. Furthermore, Niels has been a speaker at various conferences on privacy and cybersecurity, including NATO's 2nd Cyber Security Conference at a maritime training centre on Crete, Greece.

Niels Dahl-Nielsen is a member of the Danish Data Protection Association.

Daniel Kiil

Synch
Strandvejen 58
1. Sal, 2900 Hellerup
Denmark

Tel: +45 7027 8899
Fax: +45 7027 8898
Email: daniel.kiil@synchlaw.dk
URL: www.synchlaw.se/da

Daniel Kiil joined Synch in 2018 and works as a lawyer. He is specialised within IT, technology and personal data protection. Further, he has experience within corporate and intellectual property law. Daniel works with Synch's team in Scandinavia. He previously worked at Rambøll Management Consulting as a Senior Legal Consultant. Earlier, he was a lawyer at DXC Technology.

England & Wales

Nigel Parker

Allen & Overy LLP

Alexandra Rendell

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes. Under the Computer Misuse Act 1990, it is an offence to cause a computer to perform any function with the intent to secure unauthorised access to any program or data held in a computer (or enable such access to be secured). On indictment, the maximum penalty is two years' imprisonment or an unlimited fine, or both. In 2012, two separate cases were prosecuted involving unauthorised access to Facebook accounts and Facebook's computers (respectively). In the first instance, the individual was sentenced to four and eight months concurrent in a young offender institution. In the latter, the individual was sentenced to four months' imprisonment.

Denial-of-service attacks

Yes. Under the Computer Misuse Act 1990, it is an offence to do any unauthorised act in relation to a computer that a person knows to be unauthorised, with the intent of impairing the operation of any computer, preventing or hindering access to any program or the data held in any computer, impairing the operation of any program or the reliability of any data, or enabling any of the above. On indictment, the maximum penalty is 10 years' imprisonment or an unlimited fine, or both. In 2013, an individual was sentenced to two years' imprisonment in relation to denial-of-service attacks against various websites and targeting two private individuals.

Phishing

Yes. See the answer in respect of hacking.

Under the Fraud Act 2006, phishing could also constitute fraud by false representation if (for example) an email was sent falsely representing that it was sent by a legitimate firm. On indictment, the maximum penalty is 10 years' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. See the answer in respect of denial-of-service attacks.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Yes. Under the Computer Misuse Act 1990, it is an offence to make, adapt, supply or offer to supply any article intending it to be used to commit, or which may be likely to be used to commit, an offence under section 1 (see the answer in respect of hacking) or section 3 (see the answer in respect of denial-of-service attacks) of the Act. On indictment, the maximum penalty is two years' imprisonment or an unlimited fine, or both.

Identity theft or identity fraud (e.g. in connection with access devices)

Yes. Under the Fraud Act 2006, it is an offence to dishonestly make a false representation, knowing that the representation was or may be untrue or misleading, with the intent of making a gain for yourself or another or causing a loss or risk of loss to another (i.e. fraud by false representation). On indictment, the maximum penalty is 10 years' imprisonment. In 2014, an individual was convicted of offences under the Fraud Act 2006 and Computer Misuse Act 1990 (in relation to stolen bank and credit card details) and was sentenced to a total of three years' imprisonment.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Yes. This may constitute an offence under the Computer Misuse Act 1990 (such as hacking) as well as a financial crime, such as theft (under the Theft Act 1990). A breach of confidence or misuse of private information is actionable as a common law tort, but not as a criminal offence in itself.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Please see above.

Failure by an organisation to implement cybersecurity measures

Under the Data Protection Act 2018 (and the GDPR), organisations are required to implement technical and organisational measures to safeguard personal data, which may involve implementing cybersecurity measures. A failure to implement these measures is not, in itself, a criminal offence. However, the Information Commissioner's Office (**ICO**) may investigate such a failure (if, for example, an Incident occurred and this triggered an investigation) and issue an enforcement notice requiring the organisation to comply with its obligation to implement appropriate security measures. Failure to comply with such an enforcement notice is a criminal offence. The UK has adopted a similar approach in respect of enforcement of obligations to implement security measures under the NIS Regulations.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes. For certain offences under the Computer Misuse Act 1990 (such as hacking, phishing or denial-of-service attacks), the offence

will be committed where there is a "significant link to the domestic jurisdiction". This includes the person committing the offence being in the UK, the target computer being in the UK or a UK national committing the offence while outside the UK (provided in the latter instance that the act was still an offence in the country where it took place).

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

There is an exemption for certain offences under the Computer Misuse Act 1990 (such as hacking, phishing or denial-of-service attacks) in respect of an enforcement officer acting in accordance with legislation to facilitate inspection, search or seizure without a person's consent. There are no general defences under the Computer Misuse Act 1990.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Certain terrorism offences may arise in relation to cybersecurity. For example, under the Terrorism Act 2000 it is an offence to take any action designed to seriously interfere with or seriously disrupt an electronic system if this is designed to influence the government or intimidate the public or a section of the public, or for the purpose of advancing a political, religious, racial or ideological cause. In this context, offences under UK terrorism legislation also include planning, assisting or collecting information on how to commit an act of terrorism. There have been a number of prosecutions of terrorism offences that involved seizure of the suspect's computer to secure evidence of the offence.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The UK legal framework for cybersecurity is dispersed, with a number of different laws that may apply depending on the context of the Incident and the nature of the organisation involved.

- To the extent that Incidents involve personal data, the Data Protection Act 2018 will apply, alongside the EU General Data Protection Regulation (**GDPR**). The Data Protection Act 2018 specifies provisions applicable to the UK, as permitted by the GDPR, as well as setting out data protection requirements for national security and other areas of law outside EU law, such as immigration.
- In respect of telecommunications, public electronic communications network providers and public electronic communications service providers are subject to cybersecurity obligations under the Communications Act 2003.
- Public electronic communications service providers are also subject to cybersecurity obligations under the Privacy and Electronic Communications (EC Directive) Regulations 2003 (**PECR**) in respect of personal data.
- The Network and Information Systems Regulations 2018 (**NIS Regulations**) implemented the Network and Information Systems Directive into UK law (see the answer to question 2.2).
- Public companies are subject to additional governance obligations under the Companies Act 2006, Disclosure and Transparency Rules (**DTR**) in the Financial Conduct Authority (**FCA**) Handbook, Listing Rules in the FCA Handbook and the risk management and control provisions in the UK Corporate Governance Code, which can directly or indirectly relate to cybersecurity.
- The Regulation of Investigatory Powers Act 2000 (**RIPA**) governs the investigative powers of law enforcement, such as surveillance and interception of communications data. RIPA will ultimately be replaced by the Investigatory Powers Act 2016, the operative provisions of which are not yet all in force.
- The Computer Misuse Act 1990 sets out various cybercrime offences (see the answer to question 1.1) that may be prosecuted in conjunction with offences under the Theft Act 1968 or the Fraud Act 2006.
- The Official Secrets Act 1989 may also apply in respect of servants of the Crown or UK government contractors, and creates offences in relation to disclosure (or failure to secure) certain information which may be damaging to the UK's interests.
- Various common law doctrines may also apply in respect of civil actions (see the answer to question 5.1).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Cybersecurity requirements in the telecommunications sector are set out in the Communications Act 2003 (for example, in respect of maintaining the security and integrity of public electronic communications networks and public electronic communications services). These requirements apply to providers of public electronic communications networks and public electronic communications services, and include taking measures to prevent or minimise the impact of Incidents on end users and on interconnection of networks.

Financial services infrastructure providers may be regulated by the FCA and subject to the requirements in the Senior Management Arrangements Systems and Controls part of the FCA Handbook (see the answer to question 3.2). These organisations will be operators of essential services for the purposes of the Directive.

The NIS Regulations were published in the UK on 19 April 2018 and came into force on 10 May 2018. The NIS Regulations provide than an "operator of essential services" must comply with certain security duties, including a duty to notify Incidents to the relevant competent authority. The NIS Regulations identify sector-based competent authorities (for sectors covering energy, transport, health, drinking water supply and distribution and digital infrastructure) with the National Cyber Security Centre (**NCSC**) as the UK's single point of contact for Incident reporting. The NCSC will also undertake the role of the Computer Security Incident Response Team. However, the NCSC will not have a regulatory function and, in its role as the Computer Security Incident Response Team, will only respond to Incidents that arise as a result of a cyber-attack and that have been notified to it by the competent authorities. The NIS Regulations introduce a range of penalties that can be imposed by the relevant competent authority or the ICO (in the case of digital service

providers). These range from £1 million for any contravention of the NIS Regulations that the relevant authority determines could not cause an Incident, up to £17 million for a material contravention of the NIS Regulations that the relevant authority determines has caused, or could cause, an Incident resulting in immediate threat to life or significant adverse impact on the United Kingdom economy. This maximum fine is broadly aligned to the maximum level of fine under the GDPR.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the Data Protection Act 2018 (and the GDPR), if the organisation is a data controller in respect of personal data (i.e. it determines how and why personal data is processed), it will be required to implement appropriate technical organisational measures to ensure a level of security of that personal data appropriate to the risk, including the risk of accidental or unlawful disclosure of or access to that data.

The NIS Regulations also require operators of essential services and digital service providers to take appropriate and proportionate technical and organisational risk management measures, including to prevent and minimise the impact of Incidents.

Under PECR, a public electronic communications service provider must take appropriate technical and organisational measures to safeguard the security of their service and maintain a record of all Incidents involving a personal data breach in an inventory or log. This must contain the facts surrounding the breach, the effects of the breach and the remedial action taken by the service provider.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Yes. Obligations to implement effective security measures, systems and controls may conflict with Applicable Laws relating to unlawful interception of communications. Under RIPA, it is an offence to intentionally and without lawful authority intercept a communication in the course of its transmission. Interception will be lawful if: (a) both sender and recipient have consented; (b) the interception is carried out by a communications service provider for purposes connected with the operation of that service or to prevent fraudulent or improper use of that service; (c) the government has issued a warrant; or (d) the interception is authorised by other regulations.

In respect of the latter, an organisation may lawfully monitor communications of employees in certain circumstances under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (see the answer to question 7.1).

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Under the Data Protection Act 2018 and the GDPR, a data controller will be required to notify an Incident involving personal data to the ICO without undue delay and, where feasible, within 72 hours after becoming aware of it unless it is unlikely to result in risks to individuals. This notification must include: (a) a description of the nature of the Incident (including, where possible, the categories and approximate number of affected individuals and the categories and approximate number of personal data records concerned); (b) the name and contact details of a contact point where the affected individual can obtain further information (which will be the organisation's data protection officer if there is one); (c) the likely consequences of the Incident; and (d) the measures taken, or proposed to be taken, by the organisation to address the Incident and mitigate possible adverse effects. In certain circumstances, the Incident will also need to be notified to affected data subjects (see the answer to question 2.7).

Under the Data Protection Act 2018, the ICO is not permitted to publicise any information that has been disclosed to it (for example, through notification of an Incident) if that information relates to an identified or identifiable individual or business and is not already in the public domain. However, this restriction on publication will not apply in certain cases, such as if the ICO determines that publication is in the public interest. The ICO's practice is not to publicise data breach notification information unless it has taken public enforcement action in relation to the breach, or publication is necessary in the public interest (e.g. to allay public concern).

The NIS Regulations also require operators of essential services and digital service providers to report Incidents to the relevant competent authority without undue delay. The relevant authority may inform the public where public awareness is needed either to prevent or resolve the Incident, or where this would otherwise be in the public interest, but the organisation will be consulted before disclosure to the public is made to preserve confidentiality and commercial interests.

Under the Communications Act 2003, a public electronic communications network provider must notify Ofcom of a breach of security that has a significant impact on the network's operation. Further, a public electronic communications service provider must notify Ofcom of a breach of security that has a significant impact on the operation of the service.

Similarly, under PECR, a public electronic communications service provider must notify the ICO of a data breach within 24 hours of becoming aware of the "essential facts" of the breach. The notification must include: (a) the service provider's name and contact details; (b) the date and time of the breach (or an estimate); (c) the date and time the breach was detected; (d) basic information about the time of the breach; and (e) basic information about the personal data concerned.

Organisations that are regulated by the Financial Conduct Authority (**FCA**) are also required to notify the FCA of any significant failure in the organisation's systems and controls under Chapter 15.3 of the Supervision Manual of the FCA and PRA Handbooks, which may include Incidents that involve data loss. Similarly, under European Banking Authority guidelines on major Incident reporting under the revised Payment Services Directive, payment service providers are required to report major operational or security Incidents to the competent authority within four hours from the moment the Incident was first detected, with intermediate updates and a final report delivered within two weeks after business is deemed back to normal.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Organisations are permitted to voluntarily share information with other regulatory or other authorities outside the UK, or with other private sector organisations or trade associations. However, if the Incident involves personal data, any such disclosures must be made in accordance with the requirements of data protection laws. For example, disclosures to regulatory or other authorities outside the UK must comply with restrictions on cross-border transfers of personal data.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Under the Data Protection Act 2018 and the GDPR, a data controller will be required to notify affected individuals of an Incident without undue delay if the Incident involves personal data and is likely to result in a high risk to the rights and freedoms of those individuals. This notification must include: (a) a description of the nature of the Incident; (b) the name and contact details of a contact point where the affected individual can obtain further information (which will be the organisation's data protection officer if there is one); (c) the likely consequences of the Incident; and (d) the measures taken, or proposed to be taken, by the organisation to address the Incident and mitigate possible adverse effects.

Under PECR, a public electronic communications service provider must notify affected subscribers or users of an Incident without unnecessary delay if that Incident is likely to adversely affect their personal data or privacy. The service provider should provide a summary of the Incident, including the estimated date of the breach, the nature and content of personal data affected, the likely effect on the individual, any measures the service provider has taken to address the Incident and information as to how the individual can mitigate any possible adverse impact. No notification is required if the service provider can demonstrate to the ICO's satisfaction that the data that has been breached was encrypted or was rendered unintelligible by similar security measures.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Reporting obligations under data protection laws will only apply to the extent that the Incident involved personal data. IP addresses and email addresses may constitute or comprise personal data. Reporting obligations under the Communications Act 2003, PECR or FCA rules may apply regardless of the information that was subject to the Incident.

Listed companies may also be required to notify an Incident to the FCA if it would constitute price-sensitive information (see the answer to question 4.3).

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Under data protection laws (the Data Protection Act 2018, the GDPR and PECR), the relevant regulator is the ICO (https://ico.org.uk/).

Under the Communications Act 2003, the relevant regulator is Ofcom (https://www.ofcom.org.uk/).

Under the FCA Handbook, the relevant regulator is the FCA (https://www.fca.org.uk/).

Schedule 1 to the NIS Regulations identifies sector-based competent authorities (https://www.legislation.gov.uk/uksi/2018/506/schedule/1/made).

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Under the Data Protection Act 2018 and the GDPR, failure to report an Incident involving a personal data breach, or to implement appropriate security measures, can incur a fine of up to the higher of 2% of annual worldwide turnover or EUR 10 million.

Under PECR, failure by a public electronic communications service provider to notify an Incident involving a personal data breach to the ICO can incur a £1,000 fixed fine. A failure by a public electronic communications service provider to take appropriate technical and organisational measures to safeguard the security of their service can incur a fine of up to £500,000 from the ICO.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In October 2016, the ICO issued a then-record £400,000 fine to telecoms company TalkTalk for security failings that allowed a cyber-attacker to access customer data. The ICO investigation found that the attack took advantage of a technical weakness in TalkTalk's systems which could have been prevented if TalkTalk had taken "basic steps" to protect customer data.

In June 2017, the ICO issued a £100,000 fine to Gloucester City Council after it suffered a cyber-attack that allowed the attacker to gain access to financial and sensitive personal information relating to between 30 and 40 former or current staff. In this case, the "heartbleed" vulnerability was widely publicised in the media and the Council failed to apply an available patch for the affected software.

In July 2018, the ICO announced an intention to issue a fine of £500,000 to Facebook in relation to the ICO's investigation into data analytics and political campaigns. The fine relates to two breaches of the Data Protection Act 1998, one in relation to a failure to safeguard people's information, and a second in relation to transparency failings. This is the maximum fine permitted under the Data Protection Act 1998, which was the applicable regime in this instance.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Certain sectors, such as financial services and telecommunications, are more incentivised to avoid the cost and reputational impact of Incidents. In some organisations, cybersecurity practice is driven not only by compliance with Applicable Laws but also the desire to promote good "cyber hygiene" culture. For example, although there is no legal requirement to train employees in cyber risks, many organisations do and may carry out simulations (such as phishing simulations and "war games") as a matter of good practice.

Public sector organisations (such as the National Health Service) and government authorities are subject to additional reporting guidelines issued by the central government, in addition to disclosure obligations under Applicable Laws.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Financial services organisations that are regulated by the FCA are subject to the FCA Handbook, which includes Principles for Business and the Senior Management Arrangements Systems and Controls (**SYSC**). Under SYSC 3.2.6R, regulated financial services organisations are required to take reasonable care to establish and maintain effective systems and controls for compliance with regulatory requirements and standards and for countering risk that the organisation may be used to further financial crime. Further, under SYSC 3.1.1R, the organisation is required to maintain adequate policies and procedures to ensure compliance with those obligations and countering those risks. These requirements extend to cybersecurity issues. For example, the FCA has previously fined Norwich Union Life (£1.26 million) and three HSBC firms (£3 million) for failure to have adequate systems and controls in place to protect customer confidential information and manage financial crime risk.

In respect of telecommunications, public electronic communications network providers and public electronic communications service providers must take appropriate technical and organisation measures to manage risks to the security of the networks and services, including to minimise the impact of Incidents. Public electronic communications network providers must also take all appropriate steps to protect, so far as possible, the availability of that provider's network.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Directors are required, under the Companies Act 2006, to promote the success of the company for the benefit of its members as a whole and exercise reasonable skill, care and diligence in performing their role. It is up to the board of directors of each company to ensure that the board has the relevant competence and integrity to exercise these duties in view of the risk to the company as a whole, including the risk of Incidents. A failure to prevent, mitigate, manage or respond to an Incident may be a breach of directors' duties if, for example, the failure resulted from a lack of skill, care and diligence on the part of the relevant director.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

No, there are no specific requirements in this respect. However, listed companies are required, under the UK Corporate Governance Code, to set up certain committees with responsibility for specific areas, such as audits. Financial services companies may also be required to have a risk committee. These committees may, as part of their functions, conduct risk assessments that cover cyber risk. The current UK Corporate Governance Code emphasises the board's responsibility to determine and assess the principal risks facing the company. The new UK Corporate Governance Code, which will apply to accounting periods beginning on or after 1 January 2019, extends this responsibility to a robust assessment of the company's emerging risks, which would cover cyber risk.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Under the Disclosure and Transparency Rules (**DTR**) set out in the FCA Handbook, listed companies are required to disclose an Incident if the Incident amounts to inside information that may affect the company's share price. For example, theft of business-critical intellectual property is likely to be price-sensitive information.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, there are no other specific requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

There are a number of potential civil actions that may be brought in relation to any Incident, for example:

Breach of confidence. First, the information itself must have the necessary quality of confidence about it. Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it.

Breach of contract. This could take any form from a breach of a commercial contract to an employee's terms and conditions of employment.

One example may be in relation to an International Organisation for Standardization (**ISO**) compliance standard in relation to information security and risk management. Although a failure to meet such a standard is not enforced by the ISO, if a party has contractually agreed or warranted that it complies with an ISO standard, a failure to do so will be a breach of contract.

Breach of trust. A person who owes a fiduciary duty to another may not place him or herself in a situation where s/he has a personal interest that may conflict with the interest of the person to whom the fiduciary duty is owed. If an Incident is caused by an employee or a director, a breach of trust/fiduciary duty may be claimed.

Causing loss by unlawful means. A defendant will be liable for causing loss by unlawful means where s/he intentionally causes loss to the claimant by unlawfully interfering in the freedom of a third party to deal with the claimant.

Compensation for breach of the Data Protection Act 2018 (and GDPR). Individuals who suffer "material or non-material damage" by reason of any contravention, by a data controller, of any requirements of the Data Protection Act 2018 (including the GDPR) are entitled to compensation for that damage. "Non-material damage" includes distress under the Data Protection Act 2018. This does not require the claimant to prove pecuniary loss.

Conspiracy. The economic tort of conspiracy requires there to be two or more perpetrators who are legal persons who conspire to do an unlawful act, or to a lawful act but by unlawful means.

Conversion is a tort that may cover unauthorised interference with personal information and other property.

Deceit. There are four elements: (i) the defendant makes a false representation to the claimant; (ii) the defendant knows that the representation is false; alternatively s/he is reckless as to whether it is true of false; (iii) the defendant intends that the claimant should act in reliance on it; and (iv) the claimant does act in reliance of the representation and in consequence suffers loss.

Directors' duties. See the answer to question 4.1.

Dishonest assistance may be claimed where there is a fiduciary relationship and dishonest assistance has been given by a third party to the breach of trust.

Infringement of copyright and/or database rights. Copyright is infringed when a person, without authority, carries out an infringing act under the Copyright, Designs and Patents Act, such as copying the work or communicating the work to the public. Database rights are infringed if a person extracts or re-utilises all or a substantial part of a database without the owner's permission.

Misuse of private information. Similar to a breach of confidence, but removing the need for the claimant to establish a relationship of confidence. The cause of action may be better described as a right to informational privacy and to control dissemination of information about one's private life.

Negligence may be claimed where the defendant owed a duty of care to the claimant, breached that duty of care and that breach caused the claimant to suffer a recoverable loss.

Trespass is the intentional or negligent interference with personal goods. A deliberate attempt through the internet to unlawfully manipulate data on a computer may amount to trespass to that computer.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

The following are illustrations of cases that have been brought that can be said to relate to Incidents.

Breach of confidence and various economic torts

Ashton Investments Ltd v OJSC Russian Aluminium (Rusal) [2006] EWHC 2545 (Comm): there was a good arguable case justifying service out of the jurisdiction, in respect of claims for breach of confidence, unlawful interference with business, and conspiracy where a computer server in London had allegedly been improperly accessed from Russia and confidential information and privileged information viewed and downloaded.

Contract

Bristol Groundschool Ltd v Intelligent Data Capture Ltd [2014] EWHC 2145 (Ch): a contract relating to the development of computer-based pilot training materials was a "relational" contract containing an implied duty of good faith. One party had behaved in a commercially unacceptable manner in accessing the other party's computer and downloading information, but its conduct was not repudiatory.

Frontier Systems Ltd (t/a Voiceflex) v Frip Finishing Ltd [2014] EWHC 1907 (TCC): an internet telephony provider's customer whose computer network had been hacked was not liable to pay the bill incurred by unauthorised third parties.

Trespass

Arqiva Ltd & Ors v Everything Everywhere Ltd & Ors [2011] EWHC 1411 (TCC): *obiter* reference to Clerk & Lindsell on Torts (20th Edition) at paragraphs 19-02 and 17-131. At paragraph 19-02, the authors state the proposition that "one who has the right of entry upon another's land and acts in excess of his right or after his right has expired, is a trespasser". At paragraph 17-131, the authors refer to "Cyber-trespass" and say that "[w]hile the definition of corporeal personal property may normally be straightforward, questions may nevertheless arise in a number of borderline cases, in particular in respect of electronic technology. For example, it is hard to see why a deliberate attempt through the internet unlawfully to manipulate data on a computer should not amount to trespass to that computer".

Compensation for breach of the Data Protection Act 1998

Various Claimants v Wm Morrisons Supermarket PLC [2017] EWHC 3113 (QB) 2017: in the first group litigation data breach case to come before the courts, Morrisons Supermarket was found to be vicariously liable for a deliberate data breach carried out by a rogue employee, out of working hours and at home on a personal computer. The ICO had, separately, concluded an investigation into the data breach and found that Morrisons had discharged its own obligations as required under the Data Protection Act 1998 and common law. The court concluded that Morrisons had no primary liability in respect of the breach, but there was nonetheless a sufficient connection (as the

rogue employee accessed the data in question in the course of his employment) for Morrisons to have vicarious liability.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Please see the list in the response to question 5.1.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

Monitoring of employees; for example, monitoring use of email and internet access, involves processing of personal data and so the Data Protection Act 2018 (and the GDPR) will apply. The ICO's Employment Practices Code contains guidance on monitoring employees at work. The Code states that employees still have an expectation of privacy, and so monitoring should be justified, proportionate, secured and that organisations should undertake an impact assessment and ensure that the employees are notified that monitoring will take place. This notification should include details of the circumstances in which monitoring will take place, the nature of the monitoring, how the information will be used and what safeguards are in place for the employees. A failure to comply with the Code will not automatically result in a breach of the Data Protection Act 2018. However, an organisation should be able to justify any departure from the Code, and the ICO can take this into account in consideration of any enforcement action.

Under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, an organisation may lawfully monitor and record communications without consent to: (a) ascertain compliance with regulatory practices or procedures relevant to the business; (b) ascertain or demonstrate standards which ought to be achieved by employees using the telecommunications system; (c) prevent or detect crime; (d) investigate or detect unauthorised use of the telecommunications system (such as detecting a potential Incident); and (e) ensure the effective operation of the telecommunications system.

The Investigatory Powers Act 2016 amends some of the legislation relating to a business's ability to record telephone calls with its employees, but the operative provisions are not yet in force.

The Human Rights Act 1998, and in particular the right to respect for private and family life, home and correspondence, must also be considered and balanced against obligations on the organisation to implement appropriate security measures in respect of potential Incidents.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no Applicable Laws that may prevent or limit the reporting of Incidents by an employee. However, the employee would need to satisfy the whistleblowing provisions in the Employment Rights Act 1996, one of which is that the subject matter of the disclosure falls into one or more of six categories. The categories include criminal offences and breach of a legal obligation, which may be appropriate for Incidents, although may not be wide enough to cover security flaws or mere risks.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcement authorities have various surveillance powers under UK law. For example, the Police Act 1997 authorises covert entry into and interference with communications systems by the police, and similar powers are available to the security services under the Security Service Act 1989 and the Intelligence Services Act 1994.

Other powers of surveillance and interception of communications data are subject to RIPA. Under RIPA, the Secretary of State can issue an interception warrant if this is necessary for the prevention or detection of serious crime (among others), provided this is proportionate and the information could not reasonably be obtained by other means. Under the Investigatory Powers Act 2016, new warrants are available for targeted equipment interference and targeted examination, as well as bulk warrants to enable law enforcement to obtain the communications data of multiple individuals using one warrant.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Under RIPA, telecommunications service providers are required to give effect to an interception warrant to assist law enforcement. The Secretary of State may issue a notice to a specified service provider detailing the measures that the service provider must implement to establish an interception capability.

The Investigatory Powers Act 2016 includes provision for the Secretary of State to require some telecommunications operators to install permanent interception capabilities through "technical capability notices". These notices will require approval by a Judicial Commissioner, but may include equipment interference, interception capability (such as removal of electronic protection applied to data) and disclosure of data. These provisions of the Investigatory Powers Act 2016 are not yet in force, but there is some uncertainty over whether these notices could prevent a telecommunications operator from providing end-to-end encryption capabilities to end users.

Nigel Parker
Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3136
Email: nigel.parker@allenovery.com
URL: www.allenovery.com

Nigel is a partner specialising in intellectual property, data protection and privacy, commercial contracts and IT law. He is a member of the firm's Cyber Security Group and has advised clients on strategies for managing legal risk in relation to cybersecurity, including the deployment of a variety of risk management tools, on the response to attacks and dealing with regulatory authorities, and on taking pro-active steps in response to attacks.

Chambers 2015 cites Nigel as an expert in the fields of data privacy and outsourcing, describing him as "technically faultless" as well as "very practical and very good at finding solutions".

Alexandra Rendell
Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 2639
Email: alexandra.rendell@allenovery.com
URL: www.allenovery.com

Alexandra is an associate specialising in commercial contracts, data protection, intellectual property and information technology law. Alexandra advises on complex commercial arrangements for a range of clients in the technology and financial services sector, including outsourcing and service provision arrangements, licensing and IP/data exploitation.

ALLEN & OVERY

Allen & Overy is a full-service global elite law firm headquartered in London. Our commitment to help our clients deliver their global strategies has seen us build a truly global network now spanning 44 offices in 31 countries. We have also developed strong ties with relationship law firms in more than 100 countries where we do not have a presence.

We have a strong cybersecurity practice comprising a core team of 15 partners with diverse backgrounds in data protection, bank regulation, antitrust, securities laws, technology, IT, litigation, employment, IP and corporate. This spread is crucial because cybersecurity incidents frequently span a wide range of traditional legal practice areas. There is an important legal component to cybersecurity and our integrated team of diverse practitioners reflects this requirement. As a full-service global elite law firm, we are able to advise clients on all legal issues concerning cybersecurity.

France

Frederic Lecomte

Stehlin & Associes

Victoire Redreau-Metadier

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Hacking is a criminal offence pursuant to article 323-1 of the French Criminal Code (FCC) relating to unauthorised access to an automated data processing system. The punishment for fraudulent access into an automated data processing system is imprisonment and a fine of up to €60,000. When data is modified or suppressed as a result of the unauthorised access, the sanction is three years of imprisonment and a fine of up to €100,000. When the offence is committed in a public or governmental system, the sanction is raised to five years of imprisonment and a fine of up to €150,000.

Denial-of-service attacks

Article 323-2 of the FCC sanctions the impeding or slowing down of an information system. Any kind of obstruction falling within the perimeter of article 323-2 is punishable by five years of imprisonment and a fine of up to €150,000. When the offence involves a public or governmental system, the sanctions are raised to seven years of imprisonment and a fine of up to €300,000.

Phishing

Phishing is sanctioned by the following articles of the FCC and of the Intellectual Property Code:

(i) the collection of data by fraudulent, unfair or unlawful methods is sanctioned by article 226-18 of the FCC by five years of imprisonment and a fine of up to €300,000; (ii) the theft and use of a third-party identity is sanctioned by article 226-4-1 of the FCC by one year of imprisonment and a fine of up to €15,000 – the applied sanction is cumulative with the sanctions applied pursuant to (i) above; (iii) the fraud or swindle is sanctioned by article 313-1 of the FCC by five years of imprisonment and a fine up to €375,000; (iv) unauthorised introduction of data in a system, the extraction, reproduction, transmission and use of data stored in this system is sanctioned by article 323-3 of the FCC by five years of imprisonment and a fine of up to €150,000; and (v) phishing can result in an infringement of intellectual property rights, in particular on the basis of articles L.335-2, L.713-2 and L.713-3 of the French Intellectual Property Code. The owner of the reproduced or imitated website or trademark can sue the phisher for the use of his trademark on the basis of infringement. This offence is sanctioned by three years of imprisonment and a fine of up to €300,000.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

This offence can by sentenced pursuant to article 323-1 of the FCC (*see Hacking*) but also pursuant to article 323-2 of the FCC (*see Denial-of-service attacks*) and pursuant to article 323-3 of the FCC (*see Phishing*).

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Pursuant to article 323-3-1 of the FCC, the act consisting of, without a legitimate motive (in particular for research or computer security), importing, holding, offering, transferring or making available equipment, instruments, computer programs or any data designed or specially adapted to commit one or more offences mentioned in articles 323-1 to 323-3 of the FCC (*see Hacking, Denial-of-service attacks and Phishing*) is punished with the most severe sanctions.

Identity theft or identity fraud (e.g. in connection with access devices)

Pursuant to article 226-4-1 of the FCC, the act of usurping the identity of a third party is punishable by one year of imprisonment and a fine of up to €15,000.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

The offence of theft pursuant to the FCC (article 311-1) has been extended to computer theft by French courts.

French judges now consider computer data (i.e. dematerialised information), as constituting goods likely to be stolen.

Under French law, theft is punishable by three years of imprisonment and a fine of up to €45,000.

Article 226-18 of the FCC as well as articles L.335-2, L.713-2 and L.713-3 of the French Intellectual Property Code (*see Phishing*) could also be used in some circumstances.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Article L.66 of the French Post and Electronic Communications Code imposes sanctions of two years of imprisonment and a fine of up to €3,750 for any person who, by breaking wires, damaging equipment or by any other means, deliberately interrupts electronic communications.

Attacks on the fundamental interests of the nation committed by means of information technologies are punished by numerous provisions of the FCC. For example, pursuant to article L.413-10 of the FCC, the destruction, misappropriation, subtraction, reproduction of the defence secrecy or the giving of access to an unauthorised

person or making it available to the public, is sentenced to seven years of imprisonment and a fine of up to €100,000.

Failure by an organisation to implement cybersecurity measures

The failure by an organisation to implement cybersecurity measures does not constitute a criminal but an administrative offence, and the organisation would be subject to administrative fines and civil liability. Pursuant to the GDPR and the new French Data Protection Act (FDPA) n° 78-17 of January 6, 1978 (amended by the GDPR), the administrative fine imposed by the French data controlling body (the CNIL) can be up to €20 million or 4% of the company's worldwide consolidated annual turnover.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Pursuant to article 113-2-1 to the FCC, any crime or offence committed by means of an electronic communication network is deemed to have been committed on the territory of the Republic when it is attempted or committed to the detriment of a natural person residing on the territory of the Republic or a legal person whose registered office is in France.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

An offence will only be sanctioned by a court pursuant to the FCC if the intentional nature of the offence results from the facts or is demonstrated by the prosecutor. Pursuant to the GDPR as applied under French law, the lack of intentional motivation, all measures taken by the controller or the processor to mitigate the damage suffered by the data subjects, and/or the degree of cooperation to remedy the breach are considered as positive behaviour and may reduce the level of administrative sanctions. As a general principal, the level of sanction is left to the appreciation of the CNIL or the judge and will mainly depend on the situations and the behaviour of the charged party.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Many of the FCC provisions may apply or be linked to cybercrime. For example, article 226-16 to 226-24 set out the criminal offences for the violations of the FDPA. With respect to terrorism article 322-6-1 of the Criminal Code, it provides that: "*The act of disseminating by any means, except to professionals, processes allowing the manufacture of destruction devices shall be punishable by three years' imprisonment and a fine of €45,000. The penalties are increased to five years' imprisonment and a fine of €75,000 where an electronic communication network has been used for the dissemination of the processes to an unspecified public*." Moreover, article 421-2-5-1 of the same code sentences with five years of imprisonment and a fine of €75,000 the act of extracting, reproducing and intentionally transmitting data that intentionally promotes acts of terrorism.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The most important laws in the cybersecurity domain are (without being exhaustive):

- The Law Godfrain (*n°88-19 of January 15, 1988*).
- The FDPA (*Loi Informatique et Libertés n°78-17 of January 6, 1978*) successively amended by two laws: the law for confidence in the digital economy (*Loi pour la confiance dans l'économie numérique, n° 2004-575 of June 21, 2004*); and finally amended by the *Law n°2018-793 of June 20, 2018* transposing the GDPR.
- The Law for a Digital Republic (*Loi pour une République numérique, n° 2016-1321 of October 7, 2016*) and recently amended by the law transposing the GDPR (*Law n°2018-493 of June 20, 2018*).
- The Network and Information Systems Security Act transposing the NIS Directive (*Loi sur la sécurité des réseaux et systèmes d'information, n°2018-133 of February 26, 2018*).

In addition to the abovementioned law, the following texts have adapted the criminal law to certain forms of cybercrime and creating specific investigative means such as:

- The Law on Daily Security (known as LSQ *n° 2001-1062 of November 15, 2001*), *the Law on Internal Security* (*n°2003-239 of March 18, 2003*).
- The law adapting the judiciary to developments in crime (*n° 2004-204 of March 9, 2004*), the Law on Copyright in the Information Society (known as *David's Law of August 1, 2006, n°2006-961*).
- The Law OPSI II (*n° 2011-267 of March 14, 2011*).
- The Law strengthening the provisions on the fight against terrorism (*n° 2014-1353, of November 13, 2014*).
- The Law strengthening the fight against organised crime and terrorism (*n° 2016-731, of June 3, 2016*).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

In France, critical infrastructures identified as such by the law (*Law n°2013-1168 of December 18, 2013, Law n°2018-133 of February 26, 2018, Law n°2016-41 of January 26, 2016*) must comply with specific legal requirements. This is mostly the case for the following infrastructures:

- Professionals subject to the obligation of professional secrecy. For instance, pursuant to article 1111-8-2 of the French Public Health Code, healthcare institutions as well as bodies and services carrying out prevention, diagnosis or care activities shall report without delay serious information system security Incidents to the Regional Health Agency. Moreover, pursuant to article 1111-8 of the same code any person who hosts personal health data, must be accredited by the National Health Accreditation Authority for this purpose.

- Essential operators for essential services (i.e. infrastructure in the energy, transport, banking, financial market, drinking water supply and distribution and digital infrastructure sectors).
- Digital service provider.

The Network and Information Systems Directive has been implemented in France by the Law 2018-133 of February 26, 2018 about the security of networks and the information system. Pursuant to article 9 of this new law, these infrastructures must implement technical and organisational measures to prevent and reduce the impact of Incidents, identify the IT security risks that may affect their activities (failing which they incur a fine up to €100,000) and notify the ANSSI (National Agency for IT system Security) about the security Incidents they suffer (failing which they incur a fine of up to €75,000).

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Pursuant to the GDPR, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the identified risk.

Pursuant to article 34 of the FDPA, the controller (and processor) are required to take all necessary precautions, having regard to the nature of the data and the risks associated with the processing, to preserve the security of the data and, in particular, to prevent it from being distorted, damaged or accessed by unauthorised third parties.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Such conflicts may arise in France, for example, concerning the storage period of personal data (storage periods within the meaning of the FDPA may conflict with the rules of proof). Such conflicts may also arise with countries that are not a member of the European Union.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

The GDPR (article 33) provides for an obligation for all data controllers to notify any Incidents to the competent data controlling body unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. This notification to the controlled body must take place within 72 hours of the discovery breach and must contain a description of the Incident, an indication of the category of the affected data, the concerned data subjects, a detailed description of the measures taken to remedy or mitigate negative effects and the name and contact details of the data protection officer. The notification to the competent data protection authority must also describe possible harmful consequences of the unlawful access and measures taken by the controller.

The FDPA (article 34*bis*) which specifically concerns the Internet Service Providers (ISP) provides for an obligation to notify any data breach to the CNIL immediately and without conditions (the likelihood that the Incident may cause a risk to the rights and freedoms of natural persons is not required). The information to be communicated is rather similar to the abovementioned.

Finally, pursuant to article 9 of the law 2018-133 of February 26, 2018, about the security of networks and information system, critical infrastructures also have the obligation to notify security breaches to the ANSSI.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

It is possible to voluntarily notify such security breaches to other competent authorities.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Pursuant to the GDPR and the FDPA, if the breach creates a high risk to the rights and freedoms of affected individuals (article 34 of the GDPR) and/or if the breach creates a risk compromising the personal data or privacy of the person concerned (article 34*bis* of the FDPA) the controller shall have the obligation to inform each affected individual of any security breaches.

The information must detail the name and contact details of the data protection officer (DPO) and describe in clear and plain language the nature of the personal data breach, describe the likely consequences of the personal data breach and the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The GDPR covers three cases where such notification is not necessary (e.g. the implementation of post-breach measures to ensure the absence of a high risk).

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

None of these cases would change the responses to questions 2.5 to 2.7.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The CNIL controls the proper application of the FDPA and the GDPR by data controllers and processors. It also gives opinions on legislative drafts or regulatory texts.

The CNIL has important powers of control and investigation.

Finally, the CNIL has significant administrative and financial penalty powers and can take decisions such as the temporary or permanent suspension of data processing.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Depending on the nature of the offence, the penalty may vary between €10 million or 2% of the worldwide turnover, and €20 million or 4% of the worldwide turnover.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Since the entry into force of the GDPR, the CNIL has sanctioned several companies for various reasons. For example, the CNIL fined a French association €75,000 for inadequately protecting users' data on its website. The CNIL also fined OPTICAL CENTER €250,000 for not having sufficiently secured the data of their online customers on its website.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The measures to be implemented are stronger in some business areas. This is particularly the case for critical infrastructures which must comply with the law of February 26, 2018 transposing the NIS Directive (*see* question 2.2), or for Infrastructures that process sensitive data (for example, health data or data relating to criminal sentences, offences or security measures). Also, as mentioned above (*see* question 2.2), companies who host personal health data must be accredited for this purpose.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The legal requirements related to cybersecurity in the following two sectors are as follows:

(a) The financial services sector must comply with several requirements such as auditing IT systems, strengthening resistance to cyber risks, developing defences adapted to the complexity of cyber-attacks, and making several declarations to the ANSSI (ministerial orders of November 28, 2016).

(b) Pursuant to article L33-1 of the French Post and Electronic Communications Code, companies in the telecommunication sector must comply with rules relating to the conditions of permanence, quality, availability, security and integrity of the network and service, which include obligations to notify to the competent authority breaches to the security or integrity of networks and services.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Beyond the company's responsibility in case of failure of the IT system (*see* question 2.10), the company manager (i.e. in France, it is the representative of the company who has the power to bind the company, e.g.: president; CEO; and general manager) is liable under civil law towards the company and its shareholders of (i) breach of the laws and regulations or of the bylaws, and (ii) mismanagement (article 1850 of the Civil Code). Moreover, the company manager can be liable because of the behaviour of his employees if such behaviour results in damage to a third party (article 1242 paragraph 5 of the French Civil Code). Finally, French law provides numerous criminal offences which may apply to the manager of a company. Actually, pursuant to the FCC but also the French Commercial Code there are numerous provisions specifically making the company manager subject to personal criminal liability.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Please see below the Applicable Law requirements:

(a) There are no general obligations, so far, to designate a CISO. However, the GDPR sets out the obligation to appoint a DPO when (i) the data processing is carried out by a public authority or public body, (ii) the data processing requires regular and systematic monitoring on a large scale, and (iii) in cases of large-scale processing of sensitive data. Concerning the designation of the DPO, French law strictly applies the GDPR (unlike other European Union Member States, such as Germany). Consequently, apart from the three cases mentioned above, the designation of a DPO is optional in France.

(b) For the critical infrastructure, several ministerial orders of November 28, 2016 (article 10) set out the obligation to maintain a crisis management procedure in the event of major cyber-attacks. For other companies, there are no general obligations to establish a written Incident response plan or policy.

(c) Pursuant to the FDPA (article 70-13), the controller and the processor must carry out a risk assessment in order to implement measures to protect data processing systems. Moreover, pursuant to article 1110-4-1 of the French Public Health Code, health professionals, healthcare institutions and services must use information systems for the processing of health data, their storage on electronic media and their transmission by electronic means, in accordance with interoperability and security standards in order to guarantee the quality and confidentiality of personal health data and their protection.

(d) For critical infrastructures, the ministerial orders of November 28, 2016 impose audits to assess the level of security of

information systems with regard to known threats and vulnerabilities. For other companies, the French law strictly applies the GDPR according to which the controller and the processor must implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (article 32.1.d).

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Pursuant to article L.225-100-1 of the French Commercial Code and article 222-3 of the General Regulations of the French Financial Markets Authority, listed and private companies must draw up an annual management report which contains a description of the main risks and uncertainties the company had to face or is facing (which implicitly includes cyber risks). Pursuant to article L.451-1-2 of the French Commercial Code, listed companies are required to submit this report to the French Financial Markets Authority and to publish it on their website.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

To the extent that they fall within the scope of the NIS Directive and/or the GDPR, public and listed companies are subject to the requirements of these texts.

In addition, public sector infrastructures are subject to the RGS (the general security database), which aims at securing electronic exchanges from the public sphere by ensuring that the level of security of these information systems is well adapted to the challenges and risks involved (Article 1 of *Decree n°2010-112 of February 2, 2010*).

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Under French Law the general rule of civil liability is set forth under article 1240 of the French Civil Code pursuant to which any act which causes damage to another shall oblige the person by whose fault it occurred to repair it (i.e. three elements are necessary to engage liability: (i) a fault; (ii) a damage; and (iii) a causal link between the two). Moreover, under the GDPR (article 79) a civil action may be brought in the event of an Incident if the controller or the processor have not complied with the GDPR requirements. Finally, under the FDPA, the data subject shall have the right to mandate a not-for-profit body, organisation or association to stop the breach and to obtain compensation (article 43*ter*).

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

There are several examples of cases that have been brought to French courts in the relation to Incidents. For example, a woman was penalised in civil and criminal terms by the Chambery Court of Appeal on November 16, 2016 for the possession of hacking data. Another example, is where on August 12, 2016, the Paris Regional Court sentenced in civil and criminal terms a man for usurping a digital identity.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

See the answers to questions 5.1 and 5.2.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Cyber risk is partially covered by traditional insurance contracts which cover certain foreseeable consequences of certain computer threats (e.g. insurance contracts covering damage to property and civil liability). The emergence of new risks from the evolution of technologies and the increase in their uses has required and still requires the implementation of appropriate legal frameworks. To cope with these new risks, insurers have developed a new contract: the cyber contract; which is a multi-risk contract cover for damage (costs and losses incurred) and liability (non-material damage to third parties); and management services of crisis.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Pursuant to article L.113-1 of the French Insurance Code, the insurer does not cover loss or damage resulting from the insured's intentional or wilful misconduct. In addition, criminal sanctions are not insurable because they are regarded as personal sanctions. Moreover, there is still a debate about the possibility to insure administrative or financial sanctions (such as the one provided by the GDPR) to the extent they are not the result of intentional misconducts. The authors opine that this risk should be insurable.

On the subject of terrorism and cyberterrorism, the French Public Purse stated that "*insurance contracts whose purpose is to guarantee the payment of a ransom to Daech, as to any terrorist entity, are prohibited*".

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The specific requirements under the Applicable Law are as such:

(a) The monitoring of employees is authorised. Actually, the employer can control and limit the use of the Internet (site filtering devices, virus detection, etc.) and e-mail (tools for measuring the frequency of messages sent and/or the size of messages, "anti-spam" filters, etc.). The purpose of this control is to ensure the security of networks that could be attacked (viruses, Trojans, etc.) and to limit the risks of abusive or personal use of the Internet or e-mail. However, (i)

the introduction of a monitoring process to monitor employee activity requires a prior information and consultation of the employee representative committee and (ii) an individual information for employees. As a consequence, the monitoring must be proportionate, i.e. respect the balance between the employee's private life and the employer's power of control.

(b) Except for the DPO, there is no specific statutory obligation for employees to report such risks to their employer. However, internal policies (such as company rules or an IT security charter) can encourage employees to adopt a proactive reporting behaviour if they noticed an Incident. In France, there is also a "whistleblowing" mechanism available to employees (this can be, for example, an "ethical line" telephone number or a specific e-mail address). This system enables employees to report problems that could seriously affect a company's activity or seriously engage its liability. However, this mechanism remains optional. An employee cannot be sanctioned if he does not use it.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no Applicable Laws that may prohibit or limit the reporting.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In France, there are many police services specialising in cybersecurity. For example: the PICyAN (Cybercrime investigation platform and digital analysis), which analyses IT equipment seized during police searches and Internet surveillance thanks to special software; the C3N (Digital Crime Centre) whose mission includes judicial investigations and criminal intelligence; the BEFTI (Information Technology Fraud Investigation Brigade), which operates only in Paris and the surrounding suburbs and which is responsible for managing any breaches of the data processing system, software counterfeiting and classic offences such as fraud; and the OCLCTIC (Central Office for the Fight against Information and Communication Technologies Crime), which ensures the legality of published content on Internet and ordering providers to remove illegal content.

The police services mentioned above may carry out investigations, searches, interceptions, data collection, geolocation, wiretapping, infiltration, and arrest and detain suspects in police custody.

In addition, in order to ensure the effective application of the FDPA and the GDPR, the CNIL has the power to carry out extensive controls on all data controllers and processors. These controls can take place in the controlled entity's facilities, on documents, on audition or online.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There is no obligation to set up backdoors. However, the administrative and judicial authorities may require the submission of encryption keys. Actually, pursuant to article L.871-1 of the French Internal Security Code, natural or legal persons who provide encryption services aimed at ensuring a confidentiality function are required to submit within 72 hours to authorised agents (i.e. administrative and judicial authorities) at their request, agreements enabling the decryption of data transformed by means of the services they have provided. Article 434-15-2 of the FCC provides that any person who has knowledge of the secret agreement to decrypt a cryptology means that may have been used to prepare, facilitate or commit a crime or offence who refuses to surrender the said agreement to the judicial authorities or to implement it at the request of these authorities is subject to three years of imprisonment and a fine of up to €270,000.

Frederic Lecomte
Stehlin & Associes
48 avenue Victor Hugo
Paris, 75116
France

Tel: *+33 1 44 17 07 70*
Fax: *+33 1 44 17 07 77*
Email: *f.lecomte@stehlin-legal.com*
URL: *www.stehlin-legal.com*

Frederic Lecomte has been a member of the Paris Bar since 1989. Frederic joined Stehlin & Associes in 1993 after having spent five years at Coudert Brothers in Paris. He became a partner in 1998.

Frederic is the author of numerous articles in relation to technology law and is the author of a book about the GDPR *Nouvelle Donne Pour les Données* (Fauve Editions, 2018).

Practice areas: new technologies and data law; intellectual property; contract law and trade; and distribution law.

Victoire Redreau-Metadier
Stehlin & Associes
48 avenue Victor Hugo
Paris, 75116
France

Tel: *+33 1 44 17 07 70*
Fax: *+33 1 44 17 07 77*
Email: *v.redreaumetadier@stehlin-legal.com*
URL: *www.stehlin-legal.com*

Victoire Redreau-Metadier has been a member of the Paris Bar since 2017. Victoire joined Stehlin & Associes in 2017.

Victoire was involved in the writing of the book about the GDPR *Nouvelle Donne Pour les Données* (Fauve Editions, 2018).

Practice areas: new technologies and data law; intellectual property; contract law and trade; and distribution law.

Stehlin & Associés

Stehlin & Associes is an independent business law firm that was founded in 1989.

The firm's attorneys work together in a pragmatic way to implement their projected operations and solve problems encountered by clients, both in their day-to-day business as well as in specific transactions. With an international outlook from the beginning of its existence, the firm has numerous contacts with firms throughout the world. Since 2012, the firm has been the French member of the Mackrell International network, which is ranked among the top law firm networks in *Chambers* 2018, with a presence in 60 countries and 170 cities, and providing access to more than 4,500 attorneys.

Our team assists its clients in the new technologies and intellectual property fields, which include copyright and neighbouring rights, industrial property rights, Internet and new technologies rights and Privacy law.

Germany

Dr. Alexander Niethammer

Eversheds Sutherland

Steffen Morawietz

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

All of the following activities constitute a criminal offence in Germany.

Hacking (i.e. unauthorised access)

Hacking constitutes a criminal offence according to Sec. 202a of the German Criminal Code (so-called "unauthorised obtaining of data"). According to this provision, whosoever unlawfully obtains data for himself, or another, that was not intended for him and was especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine.

Denial-of-service attacks

Denial-of-service attacks constitute a criminal offence according to Sec. 303b of the German Criminal Code (so-called "computer sabotage"). According to this provision, whosoever interferes with data processing operations which are of substantial importance to another by deleting, suppressing, rendering unusable or altering data, or by entering or transmitting data with the intention of causing damage to another, shall be liable to imprisonment for up to three years or a fine. The same applies to destroying, damaging, rendering unusable, removing or altering a data processing system or data carrier. Also, it is important to note that the sole attempt is punishable and if the data processing operation is of substantial importance for another's business or enterprise, or a public authority, the penalty can be imprisonment for up to five years or a fine.

Phishing

Phishing can constitute two different criminal offences. The unlawful interception of data by technical means from a non-public data processing facility constitutes a criminal offence according to Sec. 202b of the German Criminal Code and is punishable with imprisonment for up to two years or a fine. The *use* of such data with the intent of obtaining an unlawful material benefit would constitute a criminal offence under Sec. 263a of the German Criminal Code (so-called "computer fraud") and is punishable with imprisonment for up to five years or a fine.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Infection of IT systems with malware constitutes a criminal offence according to Sec. 303b of the German Criminal Code (so-called "computer sabotage"). According to this provision, whosoever interferes with data processing operations which are of substantial importance to another by deleting, suppressing, rendering unusable or altering data, or by entering or transmitting data with the intention of causing damage to another, shall be liable to imprisonment for up to three years or a fine. The same applies to destroying, damaging, rendering unusable, removing or altering a data processing system or data carrier. Also, it is important to note that the sole attempt is punishable and if the data processing operation is of substantial importance to another's business or enterprise, or a public authority, the penalty can be imprisonment for up to five years or a fine.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

The sole possession of hardware, software or other tools which can be used to commit cybercrime can constitute a criminal offence according to Sec. 202c of the German Criminal Code. According to this provision, the preparation of the commission of an unauthorised obtaining of data or phishing by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible software for the purpose of the commission of such an offence shall be liable to imprisonment for up to one year or a fine. In case of a use of such instruments, the same principles as set forth above with respect to "Hacking" apply.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity theft can constitute various criminal offences, depending on how the offender obtains access to the identity data. This can either be done by phishing methods, which would constitute a criminal offence under Sec. 202b of the German Criminal Code as set forth above with respect to "Phishing", or by use of such identity data for fraudulent purposes, which could constitute a criminal offence under Sec. 263 of the German Criminal Code (fraud) or Sec. 263a of the German Criminal Code (computer fraud); both are subject to imprisonment for up to 10 years.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft only constitutes a criminal offence under the preconditions of Sec. 202a of the German Criminal Code. Therefore, the affected data must be especially protected against unauthorised access. Usually, this is not the case when a current or former employee breaches confidence, as the employee has authorised access

to the data. If this is not the case and the employee circumvents the protection, this would constitute the criminal offence of "phishing". The above-mentioned principles would apply.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Under German criminal law, some other activities in connection with the above-mentioned crimes constitute criminal offences. These are: (i) *preparing* of an unauthorised obtaining or interception of data, Sec. 202c of the German Criminal Code; (ii) handling of stolen data, Sec. 202d of the German Criminal Code; (iii) violation of postal and telecommunications secrets, Sec. 206 of the German Criminal Code; (iv) computer sabotage, Sec. 303b of the German Criminal Code; (v) certain types of violation of the EU General Data Protection Regulation with the intention of enrichment or to harm someone, Art. 84 of the General Data Protection Regulation and Sec. 42 of the German Federal Data Protection Act; and (vi) falsification of digital evidence, Sec. 269 *et seq.* of the German Criminal Code.

Failure by an organisation to implement cybersecurity measures

The failure of an organisation to implement cybersecurity measures does not constitute a criminal but an administrative offence, and the organisation would be subject to civil liability in case of negligence. The financial penalty can be up to 10 million EUR or 2% of the company's annual turnover. The civil liability depends on the damage which occurred due to the organisation's failure and is basically not limited.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The above-mentioned offences have no specific extraterritorial application. However, the application of the German Criminal Code depends on the "place of the offence". According to Sec. 9 of the German Criminal Code, an offence is deemed to have been committed in every place where the offender acted or in which the result occurs or should have occurred according to the intention of the offender. Therefore, the above-mentioned offences will be applicable both if the offender acted in the territory of Germany and in case the offence affects IT systems which are situated or used for services provided in Germany where the offender acted from outside Germany.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Yes, as a general principle, under German law, positive behaviour after a violation of a statutory provision as well as compensation for the occurred damage affect the level of penalties. However, this is at the sole discretion of the court.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

No, this is not applicable in our jurisdiction.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Cybersecurity is governed by several Acts in Germany. The main law relating to cybersecurity is the German IT Security Act (*IT-Sicherheitsgesetz*) of 25 July 2015, which amended a number of laws, in particular the German Telemedia Act (*Telemediengesetz*), the German Telecommunications Act (*Telekommunikationsgesetz*), the EU General Data Protection Regulation (*Datenschutz-Grundverordnung*), the German Federal Data Protection Act (*Bundesdatenschutzgesetz*) and the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*). Besides this, parts of cybersecurity are governed by the Banking Act (*Kreditwesengesetz*) and Securities Trading Act (*Wertpapierhandelsgesetz*). Besides this formal legislation, there are a few important informal provisions with respect to IT security in Germany. These are the BSI Basic IT Protection catalogues which are developed by the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik – BSI*), the Common Criteria for Information Technology Security Evaluation, standardised as ISO/IEC 15408, and the Control Objectives for Information and Related Technology (COBIT).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Yes, the Act on the Federal Office for Information Security provides for specific obligations for providers of critical infrastructure. The law defines the following sectors as critical infrastructure:

- Energy.
- IT and Telecommunications.
- Transport and Traffic.
- Health.
- Water.
- Nutrition.
- Finance and Insurance.

However, not all companies acting in the above-mentioned sectors are subject to the regulations regarding critical infrastructure. These apply only *vis-à-vis* companies which are of great importance to the functioning of the community or which would cause a threat of public safety when having a supply shortfall.

Even though the Act on the Federal Office for Information Security provides for the obligation of providers of critical infrastructure to provide reasonable organisational and technical precautions to prevent disruption of the availability, integrity, authenticity and confidentiality of their information technology systems, the specific duties are not specified by the Act but are subject to guidelines on IT security set out by industry associations and approved by the Federal Office for Information Security.

The Network and Information Systems Directive has been implemented with effect from 30 June 2017.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes, German and European law provides for several obligations for organisations to take measures to monitor, detect, prevent and mitigate Incidents.

In detail:

- According to Sec. 13, subsec. 7 of the Telemedia Act, telemedia providers are obliged to ensure that unauthorised access to related data is not possible. A telemedia provider in the Telemedia Act means, e.g., each operator of a website. The Telemedia Act does not provide details for measures that have to be taken by the provider. Specific requirements are, however, developed by the competent data protection authorities, e.g., with respect to the prevention of unauthorised access to websites, the data protection authorities request a SSL encryption of the related data.
- According to Sec. 109 of the German Telecommunications Act, providers of public telecommunications have to implement necessary technical measures to prevent phishing of personal data. Besides this, providers of public telecommunications are obliged to appoint a security officer and develop an adequate IT security model.
- Providers of several financial products are obliged to develop an IT-specific risk management (Sec. 25a of the German Banking Act (*Kreditwesengesetz*), Sec. 33 of the German Securities Trading Act (*Wertpapierhandelsgesetz*)).
- According to Art. 5 para. 1 (f) and Art. 32 of the General Data Protection Regulation, organisations are obliged to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

This includes in particular:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical Incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Such specific conflicts may arise with foreign laws with exterritorial reach.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes, there are specific reporting obligations with respect to Incidents under German law.

In detail:

- There is a general obligation to notify security breaches to the competent data protection authority. This applies to any kind of personal data. An exception applies where the security breach is unlikely to result in a high risk to the rights and freedoms of the data subject (Art. 33 of the EU General Data Protection Regulation).

  The report must be made without undue delay and not later than 72 hours after having become aware of the breach and has to contain a description of the Incident, an indication of the category of the affected data, the concerned data subjects and a detailed description of the measures taken to remedy or mitigate negative effects. The notification to the competent data protection authority must also describe possible harmful consequences of the unlawful access and measures taken by the body. The name and contact details of the data protection officer have to be provided as well.
- In case of a breach of critical infrastructure as defined in the Act on the Federal Office for Information Security (see above under question 2.2), the provider must notify the Federal Office for Information Security of any significant disruption to the availability, integrity and confidentiality of their information technology systems, components or processes which might lead to a breakdown or malfunction of the affected infrastructure.
- Providers of public telecommunications networks or services are obliged to report any IT breach to the Federal Network Agency. The report, which must be made immediately, has to contain a description of the Incident, an indication of the category of the affected data, the concerned data subjects and a detailed description of the measures taken to remedy or mitigate negative effects.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Yes, there is no prohibition of such voluntary reports as long as possible (confidentiality) rights of third parties are safeguarded.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes, in case of a security breach which creates a notification obligation (see above under question 2.5), the data subject must be notified as soon as (i) appropriate measures have been taken to secure the data or have not been carried out without undue delay, and (ii) a criminal enforcement is not/no longer at risk. The notification to the data subjects must describe the nature of the unlawful access and include recommendations for measures to minimise possible harm. Where notifying the data subjects would require unreasonable efforts, such notification may be replaced by a public communication or similar measure whereby the data subjects are informed in an equally effective manner (Art. 34 General Data Protection Regulation). This obligation of notification applies provided the Incident is likely to result in a high risk to the rights and freedoms of the data subject. Further exceptions apply under Art. 34, para. 3 of the General Data Protection Regulation and Sec. 29 of the Federal Data Protection Act.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, none of these scenarios would change the responses to questions 2.5 to 2.7.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The requirements identified under questions 2.3 to 2.7 are enforced by the Federal Office for Information Security, competent Data Protection Authorities and the Federal Network Agency.

In detail:

- The Federal Office for Information Security is the main authority with respect to cybersecurity in Germany. This authority should be the main contact regarding questions about preventive security measures and is responsible for receiving notifications about security breaches with respect to critical infrastructures.
- Data Protection Authorities enforce all relevant data protection laws. In Germany, each federal state has a separate Data Protection Authority.
- The Federal Network Agency enforces the telecommunications-related laws and is responsible for receiving notifications about security breaches with respect to telecommunications networks and services.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Under the German IT Security Act, non-compliance may be subject to administrative fines of up to 100,000 EUR. Non-compliance with the mentioned requirements under the General Data Protection Regulation is subject to fines up to 10 million EUR or 2% of the worldwide annual turnover, whichever is higher.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Up to now, no publicly known enforcement actions have been taken by the competent authorities in cases of non-compliance with cybersecurity requirements. The reason for this is that most of the relevant laws are rather new and the competent authorities are currently trying to develop a joint position with the industry. However, this might change in the future.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The market practice with respect to information security in Germany mainly depends on the security relevance of the concrete business; in particular, whether the sector is considered as a sector which is related to critical infrastructures and whether the business processes sensitive personal data or not. However, there are no known sector-specific deviations from the strict legal requirements.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes, in detail:

- Providers of certain financial products are obliged to develop an IT-specific risk management (Sec. 25a of the German Banking Act (*Kreditwesengesetz*), Sec. 33 of the German Securities Trading Act (*Wertpapierhandelsgesetz*)).
- According to Sec. 109 of the German Telecommunications Act, providers of public telecommunications have to implement the necessary technical measures to prevent phishing of personal data. Besides this, providers of public telecommunications are obliged to appoint a security officer and develop an adequate IT security model.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Yes, such failure may lead to a breach of directors' duties.

According to Sec. 130 of the German Administrative Offences Act (*Ordnungswidrigkeitengesetz – OWiG*), the owner or management of a company commits a misdemeanour if:

- it omits purposefully or negligently to appropriately control the company; and
- if a crime or misdemeanour was committed that could have been avoided or significantly impeded by exercising such control.

The obligation to control also includes the obligation to diligently select and monitor supervising personnel, active monitoring of the development of legal and technical standards, random inspections, and enforcement of implementation measures, etc. The owner or management of a company is obligated to organise the company in a manner that allows the company to comply with the law. Consequently, failures to prevent, mitigate, manage or respond to an Incident can constitute a breach of directors' duties if the directors failed to implement the appropriate measures to avoid such occurrences.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There are no general obligations, so far, to either designate a CISO, establish a written Incident response plan or policy, or conduct periodic cyber risk assessments. However, according to Art. 32 of the General Data Protection Regulation, such measures can be required in order to ensure appropriate IT security measures. Companies shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In particular, companies shall implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing. This has to be therefore assessed on a case-by-case basis.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Notification requirements generally exist solely with respect to security breaches (see question 2.5 above). However, with respect to publicly listed companies, sole cybersecurity risks without an Incident having occurred may trigger the obligation to disclose the cybersecurity risk in an *ad hoc* notification if the risk is likely to have an impact on the company's stock market price.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Companies are obliged to implement an IT security model. However, there are no detailed statutory provisions regarding such models.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The civil liability of a company depends on whether damage has occurred due to the organisation's failure to implement an appropriate IT security model. In this case, any individual or other company which suffered material damage can take civil actions against the company which is responsible for the Incident. This liability is basically not limited, but can be covered by insurance.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

The case law on Incidents in Germany is very rare due to the lack of the possibility of class actions in Germany.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes, civil liability in tort depends on the damage which occurred due to the organisation's failure and is basically not limited.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents and are common in Germany.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations to insurance coverage against any type of loss.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

(a) Yes, the monitoring of employees is only permissible in specific cases, e.g., in case of definite suspicion. Comprehensive monitoring measures would not be admissible. In case of works-council representation, the monitoring of employees needs to be generally agreed in a works-council agreement.

(b) There is no specific statutory obligation for employees to report such risks to their employer. However, such obligations should be imposed on the employees by the employer's internal policies (e.g., whistle-blowing policies).

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No, there are no Applicable Laws that may prohibit or limit the reporting of the above.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Depending on the type of authority (e.g., Public Prosecutor, Federal Office for Information Security, Data Protection Authority), the enforcement powers vary. However, all authorities have the power to carry out on-site investigations including accessing IT systems.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No; so far, there is no such obligation. However, the German legislator is currently debating such an obligation with respect to social media and instant messaging accounts. It is likely that such a law will come into force in 2018.

Dr. Alexander Niethammer
Eversheds Sutherland
Brienner Str. 12
80333 Munich
Germany

Tel: *+49 89 545 65 318*
Email: *alexanderniethammer@eversheds-sutherland.de*
URL: *www.eversheds-sutherland.de*

Alexander Niethammer is a Partner in the Munich office of Eversheds Sutherland and heads the Company Commercial Practice Group in Germany. He specialises in complex IT transactions, cybersecurity and data protection. Alexander has advised, for over 14 years, many Fortune 100 companies from the IT, DI, Consumer and Financial sectors on global projects.

Alexander has a dual legal qualification an as attorney-at-law in New York (USA) as well as in Germany.

Alexander was recently named by the International Law Office (ILO) as the exclusive recipient of the prestigious "Client Choice Award" 2016 as Germany's best IT & Internet counsel.

Steffen Morawietz
Eversheds Sutherland
Brienner Str. 12
80333 Munich
Germany

Tel: *+49 89 545 65 262*
Email: *steffenmorawietz@eversheds-sutherland.de*
URL: *www.eversheds-sutherland.de*

Steffen Morawietz is an Associate in the IT/IP practice at Eversheds Sutherland in Munich. His activities include providing legal advice to international companies in the areas of IT law and data protection. Steffen's advice focuses on companies in the e-commerce sector, in particular with regard to data protection, cybersecurity and consumer protection requirements, contract drafting and distribution law matters. He mainly advises international and national clients from the media, sports and consumer goods industries out of court as well as in court, in particular with regard to interim legal protection. Moreover, Steffen is appointed as a lecturer in civil and public law at Ludwig Maximilians University of Munich.

EVERSHEDS SUTHERLAND

Eversheds Sutherland is a one of the leading legal service providers in the world. Eversheds Sutherland represents the combination of two firms with a shared culture and commitment to client service excellence. We are each known for our commercial awareness and industry knowledge and for providing innovative and tailored solutions for every client.

With 66 offices in 32 countries and more than 2,400 lawyers, we partner with many of the most dynamic and successful business organisations across Africa, Asia, Europe, the Middle East and the United States, to address their most critical challenges, supporting their legal needs and unlocking their global ambitions.

Our international IT team frequently works for major corporate and public clients across the globe, and also acts for some of the world-leading IT suppliers. Our cybersecurity practice spans the full range of data protection, cyber and information security law topics.

Chapter 12

India


Prashant Mara


Devina Deshpande

BTG Legal

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

The following acts constitute offences when conducted fraudulently or dishonestly and without the permission of the owner/person in charge of the computer:

(i) accessing/securing unauthorised access to a computer resource (which includes computers, communication devices, computer networks, data, computer databases or software, etc.); and

(ii) providing assistance to any person to facilitate such unauthorised access (Sec. 43(a) and (b) Information Technology Act, 2000 ("**ITA**")).

The above offences are punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 66A, ITA).

Also, see question 1.4 below in respect of cyberterrorism and criminal trespass and question 2.2 below in respect of "protected systems".

Prosecutions:

- *Kumar v. Whiteley* (2009): the accused was sentenced to one year of rigorous imprisonment and a fine of INR 5,000 for hacking a government website, gaining unauthorised access to broadband internet and making alterations to subscriber accounts in the computer database.
- Call centre employees at Mphasis were prosecuted for securing unauthorised access to PIN codes of customers of Citi Group (a client of their call centre) and using these codes to transfer funds into their accounts (2005).

Denial-of-service attacks

- Causing disruption or denial of access to any person authorised to access any computer by any means is an offence when conducted fraudulently or dishonestly and without the permission of the owner/person in charge of such computer (Sec. 43(e) and (f), ITA).
- Punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 66A, ITA).
- Also, see question 1.4 below in respect of cyberterrorism.

Phishing

While "phishing" is not expressly defined, the following acts constitute offences:

(i) **Identity theft**: fraudulent or dishonest use of the electronic signature, password or other unique identification feature of any other person (Sec. 66C, ITA).

(ii) **Cheating by personation**: using a computer/communication device to cheat by pretending/representing to be another person or knowingly substituting one person for another (Sec. 66D, ITA).

The above offences are punishable with imprisonment of up to three years and with a fine of up to INR 100,000.

(iii) **Deceptive/misleading emails**: sending emails/messages that deceive/mislead the recipient as to the origin of such message (Sec. 66A(c), ITA).

The above is punishable with imprisonment of up to three years and a fine.

Cheating under the IPC may also be invoked (see question 1.4 below).

Prosecutions:

- Mumbai Cyber Cell registered an offence against a person who circulated misleading emails ostensibly emanating from ICICI Bank to obtain confidential information (including usernames, passwords, debit card numbers, PIN codes, etc.) from the recipient bank's customers.
- Persons were arrested for circulating emails indicating that the recipient had won a lottery prize and requiring them to deposit courier, VAT and insurance charges prior to the transfer of the "lottery winnings".

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

The following acts constitute offences when conducted fraudulently or dishonestly and without the permission of the owner/person in charge of the computer:

(i) introduction of a computer contaminant/virus; and

(ii) damage to any computer, computer system or computer network or any data, database or computer program residing therein (Sec. 43(c) and (d), ITA).

The above offences are punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 66A, ITA).

Also, see question 1.4 below in respect of cyberterrorism.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Possession of any plate (including negative duplicating equipment, block, mould, etc.) for making infringing copies of copyrighted work is punishable with imprisonment of up to two years and a fine (Sec. 65, Copyright Act).

Dishonestly receiving stolen computer resources or communication devices is punishable with imprisonment of up to three years or a fine of up to INR 100,000 (Sec. 66B, ITA).

Identity theft or identity fraud (e.g. in connection with access devices)

See "Phishing" above.

Publication of electronic signatures: (i) that are fake; or (ii) for fraudulent/unlawful purposes, is punishable with imprisonment of up to two years or with a fine of up to INR 100,000 or with both (Secs 73 and 74, ITA).

Prosecutions:

- *State of Odisha v. Jayanta Das* (2017): sentenced to six years' imprisonment and a fine on charges of forgery, identity theft and cyber pornography for creating a fake profile on a pornographic website in the name of the complainant's wife.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

The following acts constitute offences when conducted fraudulently or dishonestly and without the permission of the owner/person in charge of the computer:

(i) downloading, copying or extracting data/information from a computer resource (including any removable storage medium) (Sec. 43(b), ITA); and

(ii) charging services availed of by a person to the account of another person by tampering with/manipulating any computer (Sec. 43(h), ITA).

The above are punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 66A, ITA).

Violation of privacy by intentionally or knowingly publishing/transmitting a private image of a person without his/her consent is punishable with imprisonment of up to three years or with a fine of up to INR 200,000 or with both (Sec. 66E, ITA).

Disclosure of personal information obtained while providing contractual services, with the intent/knowledge that wrongful loss/gain will result, is punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 72A, ITA).

Criminal copyright infringement (i.e. with knowledge): knowingly using an infringing copy of a computer program, and infringement and passing off of trademarks, are punishable with imprisonment of up to three years and a fine of up to INR 200,000. In each case, an enhanced penalty is invoked upon subsequent convictions (Sec. 63 and Sec. 63B, Copyright Act and Sec. 104 of the Trade Marks Act).

Theft, cheating, fraud, dishonest misappropriation and criminal breach of trust provisions under the IPC may also be invoked (see question 1.4 below).

Prosecutions:

- *Shankar v. State* (2010): an employee caused the publication of confidential information which he obtained through unauthorised access of a computer at the office of the Directorate of Vigilance and Anti-Corruption. He was charged with securing unauthorised access to a "protected system" and breach of confidentiality and privacy.
- An employee of HSBC's BPO arm in India was arrested on charges of data theft and cyber fraud for producing forged certificates used to illegally embezzle funds (2005).

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The following acts constitute offences when conducted fraudulently or dishonestly and without the permission of the owner/person in charge of the computer:

(i) destroying, deleting, injuring, altering or diminishing the value/utility of information residing in a computer resource; and

(ii) stealing, concealing, destroying or altering computer source code (including computer commands, design and layout, program analysis, etc.) with an intention to cause damage (Sec. 43(i) and (j), ITA).

The above are punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 66A, ITA).

Knowingly or intentionally tampering (concealing, destroying or altering) with computer source documents required to be kept/maintained by law is punishable with imprisonment of up to three years or with a fine of up to INR 200,000 or with both (Sec. 65, ITA).

Prosecutions:

- *Shankar v. State* (2010) (see "Electronic theft" above): a case was also made out that by downloading, copying and causing the publication of confidential information, the accused diminished the value and utility of such information and affected it injuriously.
- The offence of tampering with computer source documents was held in the following:
  - *Bhim Sen Garg v. State of Rajasthan* (2006): fabrication of an electronic record, or committing forgery by way of interpolations in a CD; and
  - *Syed Asifuddin v. State of Andhra Pradesh* (2005): Tata Indicom employees were arrested for the manipulation of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocomm.

Failure by an organisation to implement cybersecurity measures

This is not applicable in our jurisdiction. See questions 2.10 and 5.1 below for non-penal repercussions.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, provided that the offence committed outside India involves a computer, computer system or computer network located in India (Sec. 75, ITA).

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Acts under Sec. 43 of the ITA (including hacking, denial-of-service attacks, introduction of virus, etc.) not conducted fraudulently or dishonestly will invoke the civil (and not criminal) liability of compensation of up to INR 10,000,000 for damage caused.

For trademark/copyright infringement, no damages will be payable where the defendant can prove he was unaware, and had no reasonable ground for believing that the work was trademark/copyright protected.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

The following Incidents will constitute "cyberterrorism", which are punishable with life imprisonment:

(i) unauthorised access, denial of access or introduction of a computer contaminant with the intent to threaten national

security and causing (or likely to cause) death, injuries, damage to property or disruption of essential supplies/services; and

(ii) intentionally/knowingly obtaining unauthorised access to restricted information/data which may be used to injure national security, public order, relations with foreign states, defamation, etc. (Sec. 66F, ITA).

Incidents may also invoke:

(i) Criminal offences under the IPC, such as cheating, theft, criminal breach of trust, criminal trespass, forgery of electronic records, dishonest misappropriation, etc.

(ii) Penal provisions under specialised legislations which punish publishing or transmitting obscene and sexually explicit materials (such as child pornography or indecent representation of women).

Prosecutions:

- Sedition charges were pressed against a former scientist for the hacking of an internet service provider and sending emails threatening national security to the Department of Atomic Energy (2001).
- A criminal case for cheating, theft and criminal conspiracy under the IPC was registered against hackers involved in stealing debit and credit card details using a proxy IP address (2017).
- *Dr. Prakash v. State of Tamil Nadu* (2002): sentenced to imprisonment for posting nude pictures of female patients online in contravention of the ITA, IPC and Indecent Representation of Women (Prohibition) Act, 1986.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Information technology laws

(i) Information Technology Act, 2000 ("**ITA**");

(ii) IT (Certifying Authority) Regulations, 2001;

(iii) IT (Security Procedure) Rules, 2004;

(iv) IT (Procedure and safeguards for interception, monitoring and decryption of information) Rules, 2009 ("**Decryption Rules**");

(v) IT (Procedure and safeguards for blocking for access of information by public) Rules, 2009;

(vi) IT (Procedure and safeguard for monitoring and collecting traffic data or information) Rules, 2009;

(vii) IT (Intermediaries Guidelines) Rules, 2011 ("**Intermediary Rules**");

(viii) IT (Guidelines for Cyber Cafe) Rules, 2011;

(ix) IT (Electronic Services Delivery) Rules, 2011;

(x) IT (the Indian Computer Emergency Response Team and manner of performing functions and duties) Rules, 2013 ("**CERT Rules**"); and

(xi) National Cyber Security Policy, 2013.

In addition, relevant offences under the Indian Penal Code, 1860 ("**IPC**") may also be added to offences under the ITA at the time of prosecution.

Privacy and data protection laws

IT (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**Privacy Rules**").

Note:

(a) Data (Privacy and Protection) Bill, 2017 ("**Privacy Bill**") has been tabled before Parliament. Additionally, the Supreme Court of India, in 2017, recognised the right to privacy as a fundamental right under the Indian Constitution.

(b) The government recently released a draft Digital Information Security in the Health Care Act, which is geared towards the protection of "digital health data", "personally identifiable information" and "sensitive health related information" ("**Health Information**"). This Act is currently in draft form but is intended to apply (once enforced) to all clinical establishments and entities/individuals that generate, collect and have custody of Health Information.

Reserve Bank of India ("RBI") directions/notifications

(i) RBI Notification – Cyber Security Framework in Banks (June 2016) ("**Bank Notification**").

(ii) RBI Press Release – Establishment of an Inter-Disciplinary Committee on Cyber Security (February 2017).

(iii) RBI Master Direction – IT Framework for NBFC Sector (June 2017) ("**NBFC Master Direction**").

Intellectual property ("IP") laws

(i) Copyright Act, 1957.

(ii) Patent Act, 1970.

(iii) Trade Marks Act, 1999.

Telecommunications laws

Unified License Agreement ("**ULA**") issued under the Indian Telegraph Act, 1885.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The government may declare any computer resource which affects critical information infrastructure as a "protected system" and specifically identify persons authorised to access such protected systems. Securing/attempting to secure unauthorised access to a protected system is punishable with imprisonment of up to 10 years and a fine.

The government has designated the National Critical Information Infrastructure Protection Centre ("**NCIIPC**") as the national nodal agency for critical information infrastructure protection.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Intermediaries/persons in charge of computer resources may be required by the government to provide access/assistance in respect of: (i) the interception, monitoring or decryption of information stored/transmitted through a computer resource; (ii) the monitoring and collecting of traffic data/information to enhance cybersecurity and to identify/prevent the spread of computer contaminant; and (iii) the prevention, detection, investigation, prosecution, punishment, etc. of an Incident (Secs 69 and 69A, ITA and Rule 3(7), Intermediary Rules).

Intermediaries and body corporates which store/handle/deal with personal information must implement reasonable security practices and procedures (i.e. control measures commensurate with the information assets being protected) (Rule 3(8), Intermediary Rules and Rule 4, Privacy Rules).

Persons authorised to issue electronic signatures under the ITA ("**Certifying Authorities**") must: (i) use secure hardware and software; and (ii) implement security procedures to ensure secrecy and privacy of electronic signatures (Sec. 30, ITA).

Banks, Non-Banking Finance Companies ("**NBFCs**") and insurance companies must implement a board-approved cybersecurity policy (distinct from their broader IT/IS security policy) with arrangements for continuous surveillance and vulnerability testing.

Telecom companies must, within 12 months of being licensed, create facilities to monitor intrusions, attacks and frauds on their technical facilities and provide related reports to the Department of Telecommunications ("**DOT**") (Clause 39.10(i), ULA).

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

The government's approach is to maintain access to electronic communications for itself, while ensuring protection against unauthorised access by third parties. To that extent, there is a conflict in the expectation that networks/data should be protected by a "key", but that such key should be made available to the government when requested. However, there are no inherent conflicts in legislation drafted to achieve the above.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

(a) The circumstance in which this reporting obligation is triggered

- Individuals, organisations and corporate entities must promptly report the occurrence of certain Incidents (including unauthorised access, compromise of critical systems and infrastructure, malicious code, server attacks, identity theft, denial-of-service, etc.). Service providers, intermediaries, data centres and body corporates must report Incidents within a reasonable time of the occurrence or of becoming aware of the Incident (Rule 12(1), CERT Rules, and Rule 3(9), Intermediary Rules).
- In the financial services sector, all Incidents (successful and attempted) must be reported to the RBI: (i) by banks within two to six hours; and (ii) by NBFCs within 24 hours.
- Insurance companies must report Incidents which critically affect business operations and a large number of customers to the Insurance Regulatory and Development Authority ("**IRDA**") within 48 hours of knowledge of the Incident.
- See question 2.3 above in respect of telecom companies.

(b) The regulatory or other authority to which the information is required to be reported

- Indian Computer Emergency Response Team ("**CERT-In**").
- NCIIPC (for sectors falling under "critical infrastructure").
- See (a) at question 2.5 above for sector-specific reporting authorities.

(c) The nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology)

- Reports to CERT-In must specify: (i) the time of occurrence; (ii) information regarding the affected system/network; (iii) symptoms observed (i.e. suspicious probes, denial of service, unaccounted changes in firewall rules, etc.); and (iv) the relevant technical information (i.e. security systems deployed, hosts affected, actions taken to mitigate the damage, etc.). Details regarding formats for reporting Incidents are published on the CERT-In website (www.cert-in.org.in) and are updated from time to time.
- Reports to the RBI must include: (i) details of the Incident (i.e. outage of critical IT system, theft/loss of information, etc.); (ii) actions taken; (iii) impact assessment; (iv) root cause analysis; and (v) impact of the attack, etc.

(d) Whether any defences or exemptions exist by which the organisation might prevent publication of that information

- CERT-In will not disclose any information which may lead to the identification of individuals or organisations affected by, or those reporting, cybersecurity Incidents without their written consent or pursuant to a court order (Rule 13(2), CERT Rules).

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

(a) A regulatory or other authority in your jurisdiction

Please see the response to (a) at question 2.5 above.

(b) A regulatory or other authority outside your jurisdiction

No express permission or prohibition (insofar as such disclosure does not violate privacy and data protection requirements, telecom user data or banking user data).

(c) Other private sector organisations or trade associations in or outside your jurisdiction

Same as (b) above.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Certifying Authorities must, upon an event/situation which may materially/adversely affect the integrity of its computer system or conditions under which an electronic signature was granted, use reasonable efforts to notify persons likely to be affected (Sec. 34, ITA).

While there is no legal requirement to notify data breaches to affected individuals at present, the draft Privacy Bill mandates

such notification (except where notification will impede a criminal investigation or the affected individual cannot be identified).

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The responses do not change.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

- Indian Computer Emergency Response Team.
- National Information Infrastructure Protection Centre.
- Department of Information Technology.
- Department of Telecommunications.
- National Information Board ("**NIB**").
- National Crisis Management Committee.
- National Security Council Secretariat.
- Ministry of Home Affairs.
- Ministry of Defence.
- National Disaster Management Authority.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

ITA/CERT Rules/Intermediary Rules

(i) There is no penalty prescribed for non-compliance with the mandatory reporting of Incidents. As such, a residuary penalty (of up to INR 25,000) under the ITA will apply (Sec. 45, ITA).

(ii) The licence of the Certifying Authority may be revoked for failure to maintain/follow required security standards (Sec. 25, ITA).

ULA

Telecom companies will be liable:

(i) for any inadvertent security breach: a penalty of up to INR 500,000,000; and

(iii) for any inadequate compliance with the licence, intentional omission, deliberate vulnerability, etc.: a penalty of INR 500,000,000 per breach. The licence may also be terminated and the vendor who supplied the hardware/software responsible for the breach could be blacklisted (Clause 39.10(i) and (ii); Clause 3.11(ii), ULA).

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Poona Auto Ancillaries v. Punjab National Bank (2011): money was fraudulently transferred from the complainant's account after he responded to a phishing email. The bank was found negligent due to the lack of proper security checks against fraud accounts and was ordered to pay INR 4,500,000 as compensation.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Organisations in the defence, power and other national security sectors may (on a case-by-case basis) be subject to more stringent information security requirements.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

(a) The financial services sector

- **Banks and NBFCs**
  - The RBI requires banks/NBFCs to, *inter alia*:
    (i) develop a "Cyber Crisis Management Plan" ("**CCMP**") to address potential Incidents and face emerging cyber threats such as "zero-day" attacks and remote access threats;
    (ii) create awareness among stakeholders (failing which, stakeholders will not be responsible for Incidents that occur due to their ignorance);
    (iii) banks are additionally required to: (a) set up a "security operations centre" to conduct continuous surveillance and testing for vulnerabilities; and (b) appoint a Chief Information Security Officer ("**CISO**") to identify gaps in preparedness and propose measures/controls; and
    (iv) NBFCs are additionally required to: (i) consider the use of digital signatures for high-value fund transfers; (ii) develop a mechanism for safeguarding information assets (including end-to-end encryption) in respect of mobile financial services; and (iii) develop controls and secure connections when using social media for marketing products.
- **Internet-based trading/securities using wireless technology**
  - The Securities and Exchange Board of India requires stock exchanges to:
    (i) ensure brokers implement secure end-to-end encryption for all data transmission, safety features against internal/external Incidents, two-factor authentication for login, etc.; and
    (ii) arrange periodic systems audits of broker systems and include wireless technology trading in investor awareness programmes.
- **Insurance**
  - IRDA requires insurances companies to, *inter alia*:
    (i) evolve a CCMP and create awareness about cyber threats among stakeholders;
    (ii) designate a CISO to formulate and enforce policies to protect information assets;
    (iii) constitute an "Information Security Committee" for information security management; and
    (iv) undertake measures for data and application security, Incident response planning, vulnerability assessments, penetration tests, etc.

(b) The telecommunications sector

- Vendor contracts with telecom companies must: (i) allow inspection of hardware, software, the manufacturing facility, etc. by the telecom company/DOT; (ii) allow security checks of vendor software any time; and (iii) acknowledge the DOT's discretion to blacklist vendors for security breaches.
- The DOT will constitute a five-member committee (including two cybersecurity experts) to assess breaches and determine applicable penalties.
- The DOT may mandate (as necessary) that telecom companies:
  - (i) enter into vendor agreements: (a) certifying services/software are "safe to connect" and have been checked for risks/vulnerabilities; (b) covering security measures (such as access and password control); and (c) addressing service continuity and upgradation, etc.;
  - (ii) create a forum to increase security assurance levels and share common issues; and
  - (iii) build capability and capacity (through local maintenance personnel) to maintain security of the telecom network.
- Encryption standards have been prescribed for telecom and internet service providers, and bulk encryption is expressly prohibited.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Where a company is legally subject to cybersecurity requirements (such as data storage or privacy under the ITA), the occurrence of a related Incident due to the failure of the directors to implement proper systems to comply with such requirements, or to ensure the adequacy and effectiveness of the systems, may amount to a breach of directors' duties under company law (Sec. 134, Companies Act, 2013).

Persons in charge of the conduct of business of a company will be considered guilty for any contravention by the company of the provisions of the ITA or rules (unless he is able to prove lack of knowledge of the contravention or exercise of due diligence) (Sec. 85, ITA).

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The above requirements are mandatory for banks, NBFCs (with the exception of designation of a CISO), insurance companies and telecom companies.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No specific disclosure requirements are imposed.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Listed companies/companies with over 1,000 shareholders must:

(i) provide e-voting facilities with votes recorded in an electronic registry with adequate cybersecurity; and

(ii) ensure the security of any electronic records, including: (i) protection against unauthorised access, alteration or tampering; (ii) security of computer systems, software and hardware; (iii) periodic backups; (iv) ability of computer systems to discern invalid/altered records; and (v) retrieval of readable/printable records, etc. (Rule 20 and Rule 28, Companies (Management and Administration) Rules, 2014).

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

See question 1.3 above in respect of civil liability under Sec. 43, ITA.

An organisation will be liable for damages of up to INR 50,000,000 if it fails to implement reasonable security practices and procedures to protect sensitive personal information (such as passwords, financial information, biometrics, etc.) ("**SPI**") and such negligence results in a wrongful gain or loss (Sec. 43A, ITA).

Organisations required to furnish information, records, returns, etc. or to maintain books of account/records under the ITA/rules will be liable to monetary penalties for any failure to comply (Sec. 44, ITA).

Civil suits may be brought in respect of infringement of IP rights including in respect of injunction, damages and account of profits.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Prosecution under the ITA

(i) See the *Poona Auto* case under question 2.11 above.

(ii) Compensation has been imposed for breach of privacy in a number of cases, including *Amit Patwardhan v. Rud India Chains* and *Nirmalkumar Bagherwal v. Minal Bagherwal* (both 2013), where the complainants' financial information (constituting SPI) was obtained from their respective banks without their consent and used against them in legal proceedings.

IPR infringement

(i) In *Adobe Systems Inc. v. Sachin Naik* (2010), the plaintiff was held entitled to damages of INR 200,000 and costs for software infringement.

(ii) In *Infosys Technologies v. Akhil Gupta* (2005), the plaintiff was awarded a permanent injunction against the defendant's use of the trademark/name "Infosys", along with damages of INR 300,000 and costs.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Tortious liability may arise in respect of trespass (hacking), fraudulent misrepresentation (phishing/identity theft), breach of privacy, breach of confidentiality, nuisance (denial-of-service), etc.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, cyber insurance may be taken as a standalone liability policy or as an extension under errors and omissions or professional indemnity insurance.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

This is not applicable in our jurisdiction.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

This is not applicable in our jurisdiction.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

This is not applicable in our jurisdiction.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Offences under the ITA must be investigated by police officers not below the rank of Inspector (Sec. 78, ITA). Investigatory powers include:

(i) confiscating computer systems, hardware, tape drives, etc. containing information or used to contravene the ITA (Sec. 76, ITA);

(ii) entering any public place and searching and arresting without a warrant persons guilty/reasonably suspected of committing an offence under the ITA (Sec. 80(1), ITA); and

(iii) search and seizure procedures, and issuing summons, requiring the attendance of witnesses and making arrests under the Criminal Procedure Code, 1973.

Authorised officers empowered to investigate contraventions of the ITA and rules can: (a) access and undertake searches of computer systems to obtain information/data; and (b) by order require persons in charge of the computer system to provide reasonable technical assistance (Secs 28 and 29, ITA).

Intermediaries must, upon lawful order and receipt of a written request, provide information/assistance to authorised government agencies for the investigation, prosecution and punishment of offences under Applicable Law (Rule 3(7), Intermediary Rules).

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Authorised government authorities can require information generated, transmitted, received or stored in a computer resource to be intercepted, monitored or decrypted by requiring, *inter alia*: (i) access to such computer resource; (ii) cooperation and technical assistance by intermediaries (including for installation and use of interception/monitoring/decryption equipment by the authorities); and (iii) disclosure of decryption key or provision of decryption assistance by the key holder (Sec. 69, ITA and Decryption Rules).

Consent of the provider of the SPI is not required for sharing such SPI with legally mandated government agencies for identity verification or for the prevention, investigation, prosecution, etc. of offences (Rule 6, Privacy Rules).

Telecom/internet service providers must provide the DOT with all the details of the technology employed, drawings, testing instruments, installation tools, etc. Licence conditions do not expressly require means of decryption to be provided to the government, but the language is sufficiently broad to include such access (ULA).

Prashant Mara
BTG Legal
804, Lodha Supremus
Dr. E. Moses Road, Worli
Mumbai – 400018
India

Tel: +91 22 2482 0801
+91 72 0801 2801
Email: prashant@btg-legal.com
URL: www.btg-legal.com

Prashant is a commercial lawyer specialising in strategic investments, collaborations, compliance and procurement projects – mostly cross-border. He specialises in the digital business, defence (with a focus on technology transfer and licensing) and industrial (with a focus on technology deployment) sectors. His clients include Facebook, Expedia, TripAdvisor, Fitbit, AirBnB, News Corp, Indigo, MAN group, Zeppelin, Rolls Royce, Voith and Tech Mahindra.

Prashant has spent nine years in Europe, working with top-tier law firms in France, Germany and the UK.

Over the last decade, he has worked closely, as a trusted advisor, with the in-house teams of his clients. This has equipped him to approach a transaction with strategic rationale in mind, which makes the transaction interesting and the execution effective.

Prashant is proficient in providing compliance and crisis response advice, including dispute management, and acting as the interface between his clients and the regulator.

Devina Deshpande
BTG Legal
804, Lodha Supremus
Dr. E. Moses Road, Worli
Mumbai – 400018
India

Tel: +91 22 2482 0807
+91 70 4542 9808
Email: devina@btg-legal.com
URL: www.btg-legal.com

Devina is a senior associate with BTG Legal, focusing on the digital business, defence and industrials sectors. Her experience includes cross-border and domestic private equity investments, M&A, debt capital markets, Islamic finance, investment management, fund formation, corporate governance and corporate advisory.

Devina has previously worked at a magic circle UK law firm, in their London and Dubai offices. She is dual-qualified, being admitted to practise law in India and a solicitor of the Senior Courts of England and Wales.

BTG Legal is a transactional law firm with best-of-breed technical expertise, a culture of innovation, and an unrelenting commitment to excellence.

Our team has specialist sector knowledge in key areas including:

- Defence.
- Industrials.
- Digital business.
- Energy and infrastructure.
- Life sciences.
- Retail.
- Financial services.
- Transport.

Our practices include corporate transactions, M&A, private equity, commercial contracting and procurement, regulatory advice, banking and finance, project finance, labour, fraud and anti-bribery compliance and other areas of law that are fast developing to keep up with rapid changes in technology and methods of doing business.

Our lawyers have worked in-house in large conglomerates as well as in established Indian and international law firms, bringing immense depth to the team. We work closely with Osborne Clarke, a leading international law firm, and are able to extend our global reach significantly.

Clients such as Facebook, WhatsApp, Jet Airways, Indigo Airlines, Tech Mahindra, MAN, Zeppelin, News Group, TripAdvisor, Wirecard and Leica Cameras continue to trust us with their work, given our innovative service delivery models, our understanding of their sectors and our appreciation of the challenging business environment in which they operate.

Indonesia

Enrico Iskandar

Bimo Harimahesa

Bagus Enrico & Partners

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes. Under Law No. 11 of 2008 regarding Information and Electronic Transactions, as lastly amended by Law No. 19 of 2016 ("**EIT Law**"), hacking constitutes a criminal offence, which is subject to various penalties depending on the intention and the means of hacking. In general, the EIT Law stipulates that any person who, without lawful authority or against the law, intentionally accesses another person's electronic system shall be sentenced to maximum imprisonment of six years and/or a maximum fine of Rp.600 million. As for hacking for the purposes of obtaining electronic information and/or electronic records, this criminal act is punishable with a maximum imprisonment of seven years and/or a maximum fine of Rp.700 million. Meanwhile, hacking by means of breaching, infiltrating, or breaking through security systems is punishable with a maximum imprisonment of eight years and/or a maximum fine of Rp.800 million.

Denial-of-service attacks

There is no specific provision under the EIT Law which regulates Denial of Service attacks ("**DoSA**"). However, DoSA may be classified as system interference which may result in faults in the operation of electronic systems under the EIT Law, and is punishable with a maximum imprisonment of 10 years and/or a maximum fine of Rp.10 billion.

Phishing

Generally, phishing can be considered as a fraudulent act under the Indonesian Criminal Code (*Kitab Undang-Undang Hukum Pidana* – "**KUHP**"), which is subject to a maximum of four years of imprisonment. Depending on the phishing methods being used, a phisher may also be charged with the provisions under the EIT Law. For instance, phishing through 'covert redirect', or unlawful transfer of electronic information, is punishable with a maximum imprisonment of 12 years and/or a maximum fine of Rp.12 billion under the EIT Law.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

There is no specific regulation in Indonesia which regulates the infection of IT systems with malware. However, under the EIT Law, this action may be classified as system interference. See the answer in respect of DoSA above for details on the applied sentences.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Under the EIT Law, possession of computer hardware or software that is designed or developed specifically to facilitate cybercrime is punishable with a maximum imprisonment of 10 years and/or a maximum fine of Rp.10 billion. Additionally, the restriction under the EIT Law is not only limited to possession or use only, but also stretched to the production, sale, organisation to be used, import, distribution, and even provision of such cybercrime tools.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity theft or identity fraud may be considered as unlawful manipulation of personal data with the intention of misusing a certain individual's identity. Such criminal act may be subject to Article 35 of the EIT Law and is punishable with a maximum imprisonment of 12 years and/or a maximum fine of Rp.12 billion.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Under the EIT Law, electronic theft is categorised as hacking or unlawful transfer of electronic information and/or electronic records, which shall be subject to a maximum imprisonment of nine years and/or a maximum fine of Rp.3 billion. Moreover, Law No. 30 of 2000 regarding Trade Secrets ("**Law No. 30/2000**") stipulates that breach of confidential information, including trade secrets, by an employee is punishable with a maximum imprisonment of two years and/or a maximum fine of Rp.300 million, whilst Law No. 28 of 2014 regarding Copyright ("**Copyright Law**") stipulates that criminal copyright infringement is punishable with a maximum imprisonment of four years and/or a maximum fine of Rp.1 billion.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The EIT Law also prohibits any unlawful alteration, addition, reduction, transmission, tampering with, deletion, moving, and covering of any electronic information and/or electronic records owned by another person or public. Any criminal act related to the foregoing is punishable with a maximum eight years of imprisonment and/or a maximum fine of Rp.2 billion. If such act resulted in the divulgement of confidential electronic information and/or electronic records in the public sphere with inaccurate data, the offender may be sentenced to a maximum of 10 years of imprisonment and/or a maximum fine of Rp.5 billion.

Failure by an organisation to implement cybersecurity measures

Under Indonesian law, the failure of an organisation or corporate entity to implement cybersecurity measures would not lead to the imposition of criminal sanctions. On a side note, the EIT Law stipulates that if a criminal offence in the cybersecurity sector is committed by a corporate entity, the criminal sanctions shall be applied with two-thirds of the basic sentence.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, all criminal sanctions stipulated under the EIT Law have extraterritorial application. Article 2 of the EIT Law stipulates that the EIT Law itself shall apply to any person who commits legal acts as governed by this law, both within and outside the jurisdiction of Indonesia, having legal effect within and/or outside the jurisdiction of Indonesia and that are detrimental to the interest of Indonesia.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The EIT Law provides exemptions for two actions that may not be considered as criminal offences, which are as follows:

a) data interception, if it is permitted and conducted by an authorised law enforcer for the purpose of law supremacy and national security; and

b) possession of cybercrime tools, if they are intended for research activities, testing and protection of the electronic system itself, insofar as the tools are possessed in a legal and lawful manner.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Depending on the cause of action, the occurrence of an Incident may lead to another criminal offence under Indonesian laws and regulations. For instance, unlawful manipulation of electronic information and/or electronic records for money laundering purposes is punishable with a maximum imprisonment of 20 years and/or a maximum fine of Rp.5 billion pursuant to Law No. 8 of 2010 on Eradication and Prevention of Money Laundering Crimes.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Cybersecurity

The Indonesian legal framework for cybersecurity is dispersed over a number of different regulations depending on the context of the Incidents. Nonetheless, the main reference for cybersecurity in Indonesia still refers to the EIT Law, which serves as the principal policy for electronic information in Indonesia.

Data Protection

In the event that the Incidents involves personal data, data protection provisions under Ministry of Communication and Informatics ("**MCI**") Regulation No. 20 of 2016 regarding Personal Data Protection in Electronic System ("**MCI Regulation 20/2016**") shall apply. MCI Regulation 20/2016 requires all electronic system operators in Indonesia to store any personal data in its possession in an encrypted form, although there's no further stipulation on the encryption mechanism to be implemented. Further, MCI Regulation 20/2016 covers various aspects of personal data protection including an internal policy requirement in managing personal data, a notification requirement in the event of a data breach, and a reporting obligation for cross-border personal data transfer.

In addition, Government Regulation No. 82 of 2012 regarding the Implementation of Electronic Systems and Transactions ("**GR 82/2012**") requires the electronic system operator to maintain the confidentiality, integrity and availability of personal data, for which any use and/or disclosure of personal data is based on the personal data owner's consent and approval.

Intellectual Property

The Ministry of Law and Human Rights ("**MoLHR**") and MCI jointly issued Decree No. 14 of 2015 and No. 26 of 2015, respectively, regarding the Implementation of Closing Down Content and/or User Right to Access on Copyright Infringement and/or Related Rights in Electronic Systems. The joint decree stipulates, among others, a procedure on filing a report on copyright infringement in electronic systems, a verification procedure for filed reports, as well as a procedure for closing down the content and/or access right related to copyright infringement.

Privacy of Electronic Communications

The privacy of personal electronic communications is guaranteed under Indonesian prevailing laws and regulations. Pursuant to the EIT Law, any person is prohibited to conduct any interception or wiretapping of electronic information and/or electronic records in certain computers and/or electronic systems of other persons without any consent and/or authorised by the owner. However, for law enforcement purposes, lawful interception is permitted and may be applicable.

Information Security

Depending on the sensitive data to be managed by an electronic system, it may be subject to certain information security provisions under Ministry of Communication and Informatics Regulation No. 4 of 2016 regarding Information Security Management Systems ("**MCI Regulation 4/2016**"). Please see the answer to question 2.2 for detailed information.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Under MCI Regulation No. 4 of 2016, electronic systems for public services are divided into three categories based on their risks, namely: (i) strategic electronic systems, which have a serious impact on public interest, public services, state administration continuity, or national security and defence; (ii) high-level electronic systems, which have limited impact for sectoral and/or regional interests; and (iii) low-level electronic systems, which do not fall under the categories of strategic and high-level electronic systems. Particularly for strategic

and high-level electronic systems, they are obliged to implement the SNI ISO/EIC 27001 standard and obtain an Information Security Management System Certificate. Such certification shall be issued by certification institutions that are acknowledged by the MCI. Failure to comply with this obligation will result in the imposition of administrative sanctions, i.e. a written warning and temporary suspension of their Indonesian Domain Name.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The EIT Law and its implementing regulations use the term Electronic System Operator (*Penyelenggara Sistem Elektronik* – "**ESO**"), which has the meaning of any person, state administrator, corporate entity or community that provides, manages and/or operates an electronic system, either individually or jointly, to the electronic system users for the interests of its own and/or other parties. With the broad definition of ESO, any organisations that operate an electronic system will be categorised as an ESO.

Under GR 82/2012, ESOs are required to implement several measures to protect their electronic system operational activity, among others:

- providing an audit trail for the purposes of monitoring, law enforcement, dispute settlement, verification, testing, Incident response and mitigation;
- securing the components of its electronic systems;
- having and implementing a procedure and facility for securing its electronic systems to avoid disruption, failure, and loss;
- providing a security system, which includes a system and procedure for handling and preventing any cyber threats; and
- preserving the confidentiality, integrity, authenticity, accessibility, availability, and traceability of electronic information and/or electronic records that it maintains.

Further, specifically for ESOs that are related to public services, they are required to have a business continuity plan to anticipate any disturbance or disaster, as well as locate their Data Centre and Disaster Recovery Centre ("**DC/DRC**") within the territory of Indonesia for the purposes of law enforcement, protection, and implementation of state sovereignty over its citizens' data.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Particularly on the requirement of locating a DC/DRC within the territory of Indonesia, a conflict of laws issue may arise. Under Indonesian laws and regulations, an online marketplace that facilitates financial payments and/or transactions is considered an electronic system for public services; hence its provider may be obliged to locate its DC/DRC within the territory of Indonesia. However, if the online marketplace service is globally available and the provider is incorporated in a country that prohibits storage of data in overseas territory, DC/DRC of such provider is not able to be physically located within the Indonesian territory.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

GR 82/2012 stipulates that if an electronic system failure or interference with serious effects caused by another party occurs, the ESO must secure the data and immediately report to the law enforcer or the relevant supervisory agency or sectoral regulator. However, GR 82/2012 does not further provide the nature and scope of information that is required to be reported, let alone any exemption for this requirement.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

There are no prohibitions under Indonesian law for an ESO to share information related to Incidents or potential Incidents to another party, even if such party is located outside the Indonesian jurisdiction. Nonetheless, under MCI Regulation 20/2016, if the share of information involves disclosure of personal data to overseas, the ESO must firstly coordinate with MCI or the relevant supervisory agency or sectoral regulator. Further, consent from the personal data owner must firstly be obtained prior to the proposed transfer of personal data to either within Indonesia or abroad.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Any Incidents related to breaches of personal data must be reported to the personal data owner. In conveying such report, the relevant ESO must take into account the following requirements: (i) the report must include the reason or cause for the data breach's occurrence; (ii) the report may be delivered electronically provided that the relevant personal data owner has approved such way of delivery during the collection of his/her personal data; (iii) the ESO must ensure that the personal data owner has actually received the report if the incidence of data breaches may lead to potential loss; and (iv) a written report shall be submitted to the personal data owner within 14 days after the data breach(es) came into realisation.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, the response will not change due to the inclusion of the above-mentioned information.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The following bodies are responsible: (i) the Directorate General of Application Informatics of MCI; (ii) the Cyber Body and National Encryption Agency ("**BSSN**"); (iii) the Indonesia Security Incident Response Team on Internet and Infrastructure ("**ID-SIRTII**"); and (iv) any other relevant supervisory agency or sectoral regulator based on the ESO's business field.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Administrative sanctions apply, which may be taken in the forms of (i) a warning letter, (ii) administrative fines, and/or (iii) suspension of business activity.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Enforcement actions are normally taken in the sectoral field, in particular the banking and insurance sector. We are aware of the fact that one of the insurance companies in Indonesia received a warning letter from the Financial Services Authority (*Otoritas Jasa Keuangan* – "**OJK**") to open up a data centre within the Indonesian territory. However, we have never been aware of any case in which a failure to meet the compliance requirements related to cybersecurity issues resulted in the imposition of administrative fines or suspension of business activity. Even during the Cambridge Analytica data scandal in early 2018, MCI only sent a written warning and the Indonesian Parliament sent a summoning letter to Facebook regarding the personal data breach, yet no sanctions have been imposed on Facebook.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The information security requirements under GR 82/2012 and personal data protection under MCI Regulation 20/2016 are applicable to any ESO, regardless of its business sector. The most common deviation from the requirement under GR 82/2012 is applicable for any ESOs that are not related to public services, as they are not bound to mandatorily place their DC/DRC within the Indonesian territory. In addition, banking sectors may also be exempted from such requirement, provided that an approval from the relevant supervisory agency or sectoral regulator is obtained. Please see question 3.2 below.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

(a) Financial Service

Use of information technology in the banking sector is regulated under OJK Regulation No. 38/POJK.03/2016 regarding the Implementation of Risk Management in the Use of Information Technology by Commercial Banks ("**OJK Regulation 38/2016**"). OJK Regulation 38/2016 contains stricter compliance requirements for the use of information and technology in banking sectors compared to other business sectors. The following are examples of compliance requirements under OJK Regulation 38/2016 that are related to cybersecurity matters:

- forming an Information Technology Steering Committee, which at least comprises of (i) a director who oversees the IT working unit, (ii) a director who oversees the risk management working unit, (iii) the highest officer who leads the IT working unit, and (iv) the highest officer who leads the IT user working unit;
- performing a trial of the Disaster Recovery Plan for all critical applications and infrastructures in conformity with the result of the business impact analysis, at least once, within one year;
- background check of criminal records during the recruitment of IT staff, including staff of the IT service provider, and network administrator or system administrator positions;
- the requirement to have an operational IT security procedure, which includes, among others, maintaining records of the antivirus and software versions that are being used;
- considering the formation of an Incidents Response Team in Information Security, in accordance with the bank's business complexity;
- within seven days after the event is identified, reporting any critical events, abuse, and/or criminal offences in the implementation of information technology which may and/or have caused significant financial losses and/or disrupt the bank's operational continuity, in the form stipulated by OJK; and
- the DC/DRC may be located outside the territory of Indonesia provided that an approval from OJK is obtained, which will be granted if, among others, personal data of the bank's customers and their respective transactions records are not involved.

Additionally, any electronic system operator involved in Electronic Money will be required to comply with the security standard for information systems under BI Regulation No. 20/6/PBI/2018 regarding Electronic Money ("**BI Regulation 20/2018**"). BI Regulation 20/2018 contains the following security standards:

- certification compliance and/or security standards and system reliability that are applied generally or stipulated by the Bank of Indonesia or a related agency;
- maintenance and improvement of the security technology;
- self-assessment of the information system in use at least once a year;
- conducting an information system audit by an independent security auditor at least once every three years or after any significant changes; and
- issuers of Electronic Money with a value limit of more than Rp.2,000,000 must increase their security standards through the use of two-factor authentication.

(b) Telecommunication

Telecommunication network providers are considered as ESOs for public services, and are thus required to implement the general requirements of information security under GR 82/2012. Please see the answer to question 2.3 above for the detailed requirements.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

There are no specific regulations in Indonesia which regulate the responsibility of the Board of Directors of a company to conduct all necessary actions in relation to prevent, mitigate, manage or respond to any Incidents. Nonetheless, directors are required, under Indonesian Company Law, to conduct management of the company in the best interest of the company with good faith and full responsibility. Therefore, a failure to prevent, mitigate, manage or respond to an Incident may be considered a breach of director's duties in the event that the failure resulted from the directors' fault or negligence. On a side note, specifically for the banking sector, one of the directors' duties is to establish an Information Technology Strategic Plan and Bank Policy for Implementation of Information Technology, in accordance with OJK Regulation 38/2016.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Only companies in the banking sector are imposed with the requirement to designate a CISO, submit a written Incident response, conduct a periodic assessment (including to its IT services providers), and perform a trial of their Disaster Recovery Plan.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

GR 82/2012 stipulates that if an electronic system failure or interference with serious effects caused by another party occurs, the ESO must secure the data and immediately report to the law enforcer or the relevant supervisory agency or sectoral regulator. For listed companies, there are no specific requirements to disclose cybersecurity risks or Incidents in their annual report. They may, however, be required to include the occurrence of any issues which significantly affect the listed company's performance and/or stability.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Other than in the banking and financial sectors, there are no specific requirements related to cybersecurity matters that are applicable for listed companies in Indonesia.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Any civil actions that may be brought in relation to Incidents shall be based on breach of contract or tort. Particularly for tort, the EIT Law provides an underlying provision for any person, whose rights are infringed due to the unauthorised use of his/her personal data, to lodge a claim for damages.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

In 2013, a 19-year-old boy was sentenced to six months of imprisonment and charged with a fine in the amount of Rp.250,000 after he was found guilty of hacking into the official website of the Indonesian ex-president and committing illegal DNS redirection against the website.

In 2017, a man called Adi Syafitrah (with the alias M2404) was sentenced to one year and three months of imprisonment after he was found guilty of hacking into the official website of the Indonesia Press Council.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Any liability in tort cases will be subject to the amount of damages incurred by the claimant and its relation to the wrongful act.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out an insurance policy in relation to risks of Incidents as there is no prohibition regarding this matter under the Indonesian laws.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations in providing insurance coverage against specific types of loss over Incidents.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There is no specific regulation on this matter under Indonesian law.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There is no specific regulation on this matter under Indonesian law.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

For the purpose of criminal offences in the IT sector, an investigator may conduct the following actions under the prevailing law and regulation:

a) Data Interception and Tapping

According to MCI Regulation No 11/2006 and the EIT Law, lawful interception and tapping may be conducted by an authorised law enforcer for the purpose of law supremacy, national security, and criminal investigation. As for interception of mobile telecommunication networks and fixed telecommunication networks without cable infrastructure, the technical requirements for lawful data interception is further regulated under MCI Regulation No. 8/2014.

In relation to the Eradication of Terrorism Law No. 5 Year 2018, based on sufficient preliminary evidence, an investigator may conduct the following:

- Opening, checking, and impounding letters and shipments by post or shipping services that are related to terrorism law.
- Tapping phone conversation or other communication devices that may be used for preparing, planning, and carrying out criminal acts of terrorism, and also to detect someone related to, or a network of, terrorism.

The tapping mentioned above should be approved by the head of the relevant district court based on its jurisdiction. Except in emergency situations, an investigator may conduct tapping after the approval of the head of district court. The tapping may be conducted for at most one year and can be extended once by at most one year. The resulting evidence of the tapping is confidential and may be used for the investigation of terrorism only.

b) Recording and Disclosing Any Data

Law No. 36 of 1999 regarding Telecommunication ("**Telecommunication Law**") and Government Regulation No. 52 of 2000 regarding Telecommunications Operation ("**GR 52/2000**") permit telecommunication services providers, for the purpose of criminal proceedings, to record any information delivered or received by it, as well as to provide any necessary information upon the following conditions:

- Written request from the Attorney General and/or Head of the Indonesian Police Force for certain criminal acts that are sentenced with five years' or more imprisonment, a life sentence, or the death penalty.
- Request from the lawful investigator for certain criminal acts pursuant to the prevailing laws and regulations.

The Telecommunication Law and GR 52/2000 state that any kinds of information may be recorded and disclosed for the purposes of criminal proceedings. Accordingly, this interception covers all types of communications facilitated by the relevant telecommunication services provider.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

The Telecommunication Law and GR 52/2000 stipulate that service providers must cooperate with the state during criminal proceedings by providing any necessary information. Consequently, should there be any encrypted information, the telecommunication services provider must cooperate with the law enforcer by providing the required encryption keys.

Enrico Iskandar
Bagus Enrico & Partners
DBS Bank Tower, 17th floor, Suite 1701
Jl. Prof. Dr. Satrio Kav. 3–5
Jakarta 12940
Indonesia

Tel: +62 21 2988 5959
Fax: +62 21 2988 5958
Email: enrico@bepartners.co.id
URL: www.bepartners.co.id

Enrico Iskandar is a founding partner of Bagus Enrico & Partners, a firm which advises companies in corporate and commercial transactions, with an emphasis on mergers and acquisitions, corporate restructurings, property, hotels and real estate, technology, media and telecommunications.

In his technology, media and telecommunications practices, Enrico has worked on a broad range of transactional, advisory and contentious matters, and regularly advises on regulatory issues on telecommunications, networks and satellite operations, data protection/privacy, encryption, outsourcing, IT contracts, and e-commerce (online securities, trading and advertising). Enrico's considerable experience in relation to technology, media and telecommunications has enabled him to steer investors through the inherent practical and regulatory hurdles.

As part of the recognition of his representation for multinational clients in Information Technology, Telecommunication and Media, Enrico's team has been recognised by the ***Asia Pacific Legal 500 2017 & 2018 editions*** as Indonesia's **1st Tier** law firm in the ***IT & Telecoms*** practice. He has also been selected in the ***2013, 2014, 2015, 2016, 2017 and 2018 editions*** of ***The International Who's Who Legal***, as a leading individual in the ***Information Technology*** practice, and in the ***2014*** and ***2015 editions*** in the same publication, as a leading individual in the ***Telecoms & Media*** practice.

Bimo Harimahesa
Bagus Enrico & Partners
DBS Bank Tower, 17th floor, Suite 1701
Jl. Prof. Dr. Satrio Kav. 3–5
Jakarta 12940
Indonesia

Tel: +62 21 2988 5959
Fax: +62 21 2988 5958
Email: bimo@bepartners.co.id
URL: www.bepartners.co.id

Bimo Harimahesa is a principal associate of Bagus Enrico & Partners. Mainly focusing on technology, media and telecommunication areas, Bimo has been actively involved in advisory for regulatory issues across TMT aspects including telecommunication and networks operation, data privacy protection, cloud services, and e-commerce industries.

Bimo also regularly advises the firm's clients within a wide spectrum of corporate and commercial matters on various sectors; namely, mergers and acquisitions, property, hotels and real estate, and employment, as well as advising various mainstream corporate clients.

In the TMT sector, Bimo's recent representations include advising a major US-based technology company in the preparation of a global unified warranty template for the sales of its hardware products, assisting a UK-based technology company in advising a global privacy policy for the potential rollout of its intelligent household appliance, and regulatory requirements for the provision of IPVPN services licensing in Indonesia.

BAGUS ENRICO & PARTNERS
COUNSELLORS AT LAW

Bagus Enrico & Partners ("**BE Partners**") is one of Indonesia's leading corporate and commercial law firms. Founded by professionals who are recognised for their experience in handling various notable transactions in Indonesia, BE Partners continues its growth with an equal commitment to our reputation as a "boutique practice [which] focuses on client service", and provides its domestic and international clients with high-quality advice which is commercially focused and personally delivered.

BE Partners has received recognition from the main legal market reviewers. Some of the most international and respected reviewers have placed BE Partners' team as Indonesia's leading professionals in various practices. BE Partners' reputation in diverse aspects of Indonesian law, especially in relation to corporate/commercial law, banking, finance and insurance, mergers and acquisitions, IT, media and telecommunications, energy and resources, property, hotels and real estate, as well as infrastructure, is outstanding.

Chapter 14

Ireland

Kevin Harnett

Victor Timon

Maples and Calder

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

The Criminal Justice (Offences Relating to Information Systems) Act 2017 (the "2017 Act") came into force on 12 June 2017, giving effect to Directive 2013/40/EU regarding criminal attacks against information systems.

Hacking (i.e. unauthorised access)

Hacking is an offence in Ireland, which, under section 2 of the 2017 Act, occurs when a person who, without lawful authority or reasonable excuse, intentionally accesses an information system by infringing a security measure.

Denial-of-service attacks

Denial-of-service attacks constitute an offence under the 2017 Act, captured under section 3, which provides that it is an offence when a person who, without lawful authority: intentionally hinders or interrupts the functioning of an information system by inputting data on the system; transmits, damages, deletes, alters or suppresses, or causes the deterioration of, data on the system; or renders data on the system inaccessible.

Phishing

Phishing does not, *per se*, constitute a specific offence in Ireland. However, it is possible that the activity would be caught by certain other, more general criminal legislation, depending on the circumstances (for instance, relating to identity theft or identity fraud). In this regard, see below.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Infection of IT systems with malware is also an offence, again covered by the 2017 Act. In this regard, section 4 provides that a person who, without lawful authority, intentionally deletes, damages, alters or suppresses, or renders inaccessible, or causes the deterioration of data on an information system commits an offence.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Possession or use of hardware, software or other tools used to commit cybercrime also constitutes an offence under the 2017 Act (section 6), which occurs when a person who, without lawful authority, intentionally produces, sells, procures for use, imports, distributes, or otherwise makes available, for the purpose of the commission of an offence under the 2017 Act, certain hacking tools. Such tools are described as "(i) any computer programme that is primarily designed or adapted for use in connection with the commission of such an offence, or (ii) any device, computer password, unencryption key or code, or access code, or similar data, by which an information system is capable of being accessed".

Identity theft or identity fraud (e.g. in connection with access devices)

Although there is no precise, standalone offence of identity theft or identity fraud in this jurisdiction, it can nonetheless potentially be captured by the more general offence referred to as "making a gain or causing a loss by deception" (as contained in section 6 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (the "2001 Act")). This occurs where a person who dishonestly, with the intention of making a gain for himself or herself or another, or of causing loss to another, by any deception induces another to do or refrain from doing an act. In addition, sections 25, 26 and 27 of the 2001 Act cover specific forgery offences.

Separately, under section 8 of the 2017 Act, identity theft or fraud is an aggravating factor when it comes to sentencing, in relation to "denial-of-service attack" or "infection of IT systems" offences. This is described in broad terms as being a misuse of the personal data of another person with the aim of gaining the trust of a third party, thereby causing prejudice to that person.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft is covered by the relatively broad offence of "unlawful use of a computer", as provided for in section 9 of the 2001 Act. This occurs where a person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Section 5 of the 2017 Act creates the offence of "intercepting the transmission of data without lawful authority", which occurs when a person who, without lawful authority, intentionally intercepts any transmission (other than a public transmission) of data to, from or within an information system (including any electromagnetic emission from such an information system carrying such data). This is a broad provision which potentially covers other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

With regard to penalties, in relation to offences under the 2017 Act, the penalties range from maximum imprisonment of one year and a maximum fine of €5,000 for charges brought "summarily" (i.e., for less serious offences), to a maximum of five years' imprisonment (10 years in the case of denial-of-service attacks) and an unlimited fine for more serious offences. The above offences under the 2001 Act are only tried in the Circuit Court, with "making a gain or causing a loss by deception" carrying a maximum penalty of five years' imprisonment and an unlimited fine, and forgery and "unlawful use of a computer" offences carrying a maximum of 10 years and an unlimited fine.

Owing to the very recent implementation of the 2017 Act, there have been very few (if any) prosecutions of note under this particular legislation to date. That said, Ireland's first successful prosecution for hacking took place in July 2013 on foot of charges under the Criminal Damage Act 1991. The prosecution followed a collaborative investigation between the Irish Garda Bureau of Fraud and the FBI, and involved the hacking of a major political party's website during the run-up to a national election.

There have also been a number of relatively high-profile denial-of-service attacks on large national websites over the last 12 months (those of certain governmental departments and the national lottery, to name a few), which are currently the subject of ongoing investigations. These investigations may lead to some element of prosecution under the 2017 Act in the near future.

Failure by an organisation to implement cybersecurity measures

There is no particular offence in this jurisdiction directly linked to a failure by an organisation to implement cybersecurity measures. That said, and in specific relation to personal data concerning individuals, section 71 of the Data Protection Act 2018 (the "**DPA**") provides that controllers must ensure that data is "processed in a manner that ensures appropriate security of the data, including, by the implementation of appropriate technical or organisational measures, protection against (a) unauthorised access or unlawful processing and (b) accidental loss, destruction or damage".

The Data Protection Commission (the "**DPC**") may, under its statutory powers, notify an organisation that it is deemed to have breached these obligations, and further issue an enforcement notice in this respect. It is then an offence for any controller or processor to, without reasonable excuse, fail or refuse to comply with such a notice. The maximum fine imposable in this regard is €250,000 or imprisonment for a term not exceeding five years.

1.2 Do any of the above-mentioned offences have extraterritorial application?

All of the above offences under the 2017 Act have certain extraterritorial application, and so offenders may therefore be tried in Ireland, so long as they have not already been convicted or acquitted abroad in respect of the same act, and the relevant act was committed:

(a) by the person in Ireland in relation to an information system outside of the country;

(b) by the person outside of the country in relation to an information system in Ireland; or

(c) by the person outside of the country in relation to an information system also outside of the country, if:

(i) that person is an Irish citizen, a person ordinarily resident in Ireland, or a company established or existing under Irish law; and

(ii) the act is an offence under the law of the place where it was committed.

Although broader concepts such as, for instance, the "European arrest warrant" may be of relevance for Irish prosecutors, none of the above-mentioned offences under the 2001 Act carry, in and of themselves, extraterritorial application.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Each of the above offences under the 2017 Act contain the ingredient that it was committed without "lawful authority", which is defined as either "with the authority of the owner of the system", "with the authority of a right holder of the system", or "as permitted by law". Accordingly, prosecution of these offences will require, necessarily, that such authority or lawful permission was absent.

In addition, the offence relating to "hacking" carries a further qualification, i.e., where the person or company had a "reasonable excuse". This term is, however, not defined under the 2017 Act, and so its precise application will depend on future judicial interpretation.

In addition, if a company is charged with any of the above 2017 Act offences where the offence was committed by an employee for the benefit of that company, it will be a defence for that company that it took "all reasonable steps and exercised all due diligence" to avoid the offence taking place.

Separately, it can be expected that judges will continue to take established factors into account when considering the appropriate penalty on foot of a conviction of a cybersecurity-related crime (e.g., remorse, amends, cooperation with investigators, criminal history, and extent of damage).

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

It is, for instance, an offence under section 8 of the Offences Against the State (Amendment) Act 1998 to "collect, record or possess information which is of such a nature that it is likely to be useful in the commission by members of any unlawful organisation of serious offences generally or any particular kind of serious offence". The term "serious offence" would encompass any of the above-mentioned offences (apart from failure to comply with an enforcement notice issued by the DPC), so long as the act in question is one which involves "serious loss of or damage to property or a serious risk of any such loss…or damage". The maximum sentence for this offence includes an unlimited fine and 10 years' imprisonment. To date, there does not appear to have been any prosecutions of note which have combined this particular offence with acts of cybercrime.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Apart from the above-referenced statutes in respect of criminal activity, Applicable Laws include the following:

- Data Protection: The DPA governs the manner in which personal data is collected and processed in Ireland. The DPA requires that controllers take "appropriate security

measures" against unauthorised access, alteration, disclosure or destruction of data, in particular where the processing involves transmission of data over a network. The DPA adopted the General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**") to Irish law in May 2018.

- e-Privacy: The e-Privacy Regulations 2001 (S.I. 336 of 2011), which implemented the e-Privacy Directive 2002/58/EC (as amended by Directives 2006/24/EC and 2009/136/EC) (the "**e-Privacy Regulations**"), regulate the manner in which providers of publicly available telecommunications networks or services handle personal data and require providers to take appropriate technical and organisational measures to safeguard the security of its services and report Incidents. It was intended that a revised EU e-Privacy Regulation be introduced in May 2018 to replace the existing e-Privacy Directive and e-Privacy Regulations, expanding the current regime to cover all businesses which provide online communication services. That new regulation is still in draft form and at the date of writing has not yet been finalised.
- Payments Services: The new Payments Services Directive II (Directive 2015/2366/EU), was transposed by the European Union (Payment Services) Regulations 2018 (S.I. 6 of 2018) (the "**Payment Services Regulations**") on 12 January 2018, and introduced regulatory technical standards (which were published by the European Banking Authority) to ensure "strong customer authentication" and payment service providers will be required to inform the national competent authority in the case of major operational or security Incidents. Providers must also notify customers if any Incident impacts the financial interests of its payment service users. The Payment Services Regulations superseded the previous regime which was introduced in 2009.
- The Security of Network and Information Systems Directive 2016/1148/EU (the "**NISD**") was to be transposed by EU Member States, including Ireland, by May 2018. At the time of writing, the NISD had not yet been transposed; however, following the issue of a formal notice by the European Commission in July 2018, it is expected that it will shortly be transposed into Irish law. The NISD seeks to harmonise cybersecurity capabilities across the EU and achieve a common level of network and information systems security across the EU by increasing cooperation amongst EU Member States, improving national capabilities and introducing security measures and Incident reporting obligations for certain operators of essential services.
- Other: If there is a security breach which results in the dissemination of inaccurate information, persons about whom the inaccurate data relates may seek a remedy under the Defamation Act 2009. Similarly, if information was provided in confidence and such information was leaked, there may be an action under common law for breach of confidence or negligence, in the event that a duty of care is found to have been owed.

See also sections 1 and 5.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Publicly available telecommunications networks and services are governed by the e-Privacy Regulations outlined at question 2.1 above.

The Department of Communications, Energy and Natural Resources (now, the Department of Communications, Climate Action and Environment ("**DCCE**")) published the National Cyber Security Strategy 2015–2017, which provides a mandate for the National Cyber Security Centre to engage in activities to protect critical information infrastructure. As of yet, a new strategy has not been published; however, it is expected that one will be published by the end of 2018. As matters stand, the DCCE together with the Government Taskforce on Emergency Planning and the Office of Emergency Planning in the Department of Defence operate as lead government departments for emergency situations relating to, *inter alia*, critical infrastructure.

The NISD will be introduced in Ireland by primary legislation, expected shortly, following the issue of a formal notice by the Commission (see question 2.1 above). According to the Government's Legislative Programme Spring/Summer session 2018, preliminary work is under way but no bill has been published to date and, as such, it is not yet known whether the implementing legislation will exceed the requirements of the NISD.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the DPA, controllers are required to take appropriate measures, as outlined in questions 1.1 and 2.1 above. The DPA does not detail specific security measures to be undertaken but in determining appropriate measures, a controller may have regard to the state of technological development and the cost of implementing the measures. Controllers must ensure that the measures provide a level of security appropriate to the harm that might result from a breach and the nature of the data concerned. The DPC has issued guidance which suggests the introduction of measures such as access controls, automatic screen-savers, encryption, anti-virus software, firewalls, software patching, secure remote access, back-up systems and Incident response plans.

Under the e-Privacy Regulations, providers of publicly available telecommunications networks or services are required to take appropriate technical and organisational measures and ensure the level of security appropriate to the risk presented, having regard to the state of the art and cost of implementation. Such measures shall at least ensure that personal data can only be accessed by authorised personnel for legally authorised purposes, protect personal data against accidental or unlawful destruction, loss, alteration, processing, etc., and ensure the implementation of a security policy.

The NISD, once transposed into Irish law, will require that operators of essential services take appropriate measures to prevent and minimise the impact of Incidents affecting the security of the network and information systems used for the provision of essential services with a view to ensuring continuity. Similarly, digital service providers will be required to identify and take appropriate and proportionate technical and organisational measures to manage risks posed having regard to the state of the art and take account of, *inter alia*, the security of the systems and facilities, Incident handling, business continuity management and compliance with international standards.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Applicable Laws are largely harmonised at an EU level, and as such the risk of conflicts of laws is minimised. However, the existence of

differing requirements for organisations with operations both within the EU and externally may present compliance challenges for such companies.

With regard to the confidentiality of electronic communications, it is understood that updated interception legislation is in the process of being prepared, namely the Interception of Postal Packets and Telecommunications Messages (Regulation) (Amendment) Bill. The purpose of that legislation is to update the Postal and Telecommunications Acts 1983 and 1993, which are limited in scope to postal services and traditional telecommunications providers, to regulate the lawful interception of all communications delivered over the internet.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Section 86 of the DPA contains a general personal data breach notification obligation to the DPC. Where a personal data breach occurs, the controller shall without undue delay and, where feasible, within 72 hours of becoming aware of the breach, notify the DPC of the breach. This notification shall include a description of the breach, the number or approximate number of data subjects concerned and personal data records concerned. It must also contain a list of likely consequences of the breach and measures taken or proposed to be taken to address the breach.

Where a data breach occurs that is likely to result in a high risk to the rights and freedoms of a data subject, Section 87 of the DPA requires the controller to notify the data subject to whom the breach relates. The requirement is waived where the controller has implemented appropriate measures to protect the data; in particular where the measures render the data unintelligible through encryption or otherwise to any person not authorised to access it. This notification must contain at least the same information provided to the DPC as described above.

Providers of publicly available telecommunications networks or services are required to report information relating to Incidents or potential Incidents to the DPC (to the extent that such Incidents relate to personal data breaches). In the case of a particular risk of a breach to the security of a network, providers of publicly available telecommunications networks or services are required to inform their subscribers concerning such risk without delay and, where the risk lies outside the scope of the measures to be taken by the relevant service provider, any possible remedies including an indication of the likely costs involved. In case of a personal data breach, such providers must notify the DPC without delay and where the said breach is likely to affect the personal data of a subscriber or individual, notify them also. If the provider can satisfy the DPC that the data would have been unintelligible to unauthorised persons, there may be no requirement to notify the individual or subscriber of the breach.

Under Article 16 of the NISD, once implemented, Member States must ensure that digital service providers notify the relevant competent authority (in Ireland, this is likely to be the National Cyber Security Centre) without delay of any Incident having a substantial impact on the provision of a service. The notification must provide sufficient information so that the national authority can assess the significance of same and any cross-border impact. The NISD stipulates that notification shall not make the notifying party subject to increased liability.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

See above at question 2.5 regarding the requirement to notify the DPC.

The National Cyber Security Strategy published in 2015 outlines the intention of the DCCE to deepen its partnerships with third-level institutions to aid the sharing of knowledge, experience and best practice. Moreover, the Strategy outlines the active information-sharing role between the DCCE and other public sector bodies and industry at the time (including IRISS-CERT). Under the NISD, the CSIRTs Network will be tasked with exchanging and making available, on a voluntary basis, non-confidential information concerning individual Incidents.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

See question 2.5 above.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Parties must ensure that personal data is processed (e.g., shared) in accordance with the DPA and take appropriate security measures with regard to any onward transmission of data including in the context of notifications of Incidents. Personal data includes data relating to a living individual who is or can be identified from either the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the controller. There are exemptions under the DPA such as for the processing of data which is necessary for the administration of justice or to enable the controller to comply with a legal obligation. Therefore, different considerations apply in the context of voluntary sharing of personal data relating to a breach, and mandatory reporting. For that reason, controllers should take particular care when a notification includes any personal data and take steps to anonymise data where appropriate. Additional considerations also apply in the case of 'special categories of personal data' as set out in Part 3, Chapter 2 of the DPA.

Parties must also be conscious of their contractual obligations and whether issues may arise regarding the sharing of price-sensitive or confidential information, particularly if there is no mandatory requirement to do so.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The DPC is the primary regulator responsible for enforcing the requirements outlined above. The DPC is an independent body established under the DPA.

Under the NISD, it is intended that the national competent authority will be the National Cyber Security Centre which is intended to be placed on a statutory footing.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

There is no automatic penalty for controllers under the DPA in the event of a data breach. However, if the DPC issues an information notice (requiring certain information) or enforcement notice (requiring certain action), a controller or processor must comply with same. If they do not comply, it will constitute an offence. The DPC (unlike under the previous regime) can now impose administrative fines directly as follows:

- a maximum of €5,000 or imprisonment for a term not exceeding 12 months or both on summary conviction; and
- a maximum of €250,000 or imprisonment for a term not exceeding five years or both for conviction on indictment.

The original draft of the DPA exempted public bodies from administrative fines, but following intense lobbying, the DPA now provides for fines of up to €1 million in respect of those bodies.

Further, the DPA also incorporates in Section 141 the right of the DPC, as the supervising authority, to impose fines of up to €20 million or 4% of global turnover as set out in Article 83 of the GDPR.

Under the e-Privacy Regulations, a person who commits an offence is liable on summary conviction to a fine. Furthermore, if a person is convicted of an offence, the court may order any material or data that appears to it to be connected with the commission of the offence to be forfeited or destroyed and any relevant data to be erased.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In July 2016, the ODPC (now DPC) was notified of a data breach in respect of an organisation providing retail and online services. Over a two-week period, attackers attempted various username/password combinations and gained access to certain user accounts. The attackers were able to add new payments methods to those accounts and to access personal data associated with those accounts. They attempted to withdraw users' balances. The ODPC assessed the breach and identified deficiencies in the security measures used, including insufficient measures on password policy and user authentication and insufficient control measures to validate changes to users' accounts. This was considered a breach of the then current Data Protection Acts 1988 and 2003 and recommendations were issued to the organisation to take steps to mitigate the various deficiencies. If the organisation failed to take such steps, it would face enforcement action. The company implemented multifactor passwords and a comprehensive data retention policy.

Similarly, the ODPC reported that in October 2016 a primary school was the victim of a "crypto ransomware attack" which rendered the school's files inaccessible. These files contained personal details and a ransom was demanded to release same. The school was found to be in breach of the DPA as it had not put in place appropriate security measures and had no policies or procedures to maintain adequate backups. Recommendations were issued to the school and the school implemented staff training and awareness and reassessed its contractual arrangements with its ICT suppliers.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, market practice with respect to information security varies considerably in Ireland dependent on the industry sector concerned. Businesses in industries that are recognised as being particularly vulnerable to Incidents, such as the financial services sector, are more likely to have adequate processes in place to effectively address cyber risk. With current and long-term trends, such as the continued expansion of cloud computing, mobile data and the internet of things further increasing exposure to cyber risk, financial services firms are expected to update and implement their processes accordingly. The publication of the Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks by the regulator for financial institutions, the Central Bank of Ireland, provides valuable information on the practices that financial services firms are expected to apply in order to protect their organisations from cyber threats.

Other industries have previously been less cognisant of the need for adequate cybersecurity protections. For example, the manufacturing industry in Ireland has been largely unaffected by Incidents. However, advances in robotics, technology and the digital marketplace have increased the awareness of manufacturers to the need for maintenance and protection of cyber infrastructure. In response to this, IBEC, the largest business and employer association for organisations based in Ireland, has highlighted the prioritisation of cybersecurity as a key component in the development of the manufacturing industry in Ireland and has set out a number of recommendations in a recent report setting out their short- to medium-term strategy for Ireland's manufacturing industry.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

(a) There is currently no specific legislation focused on cybersecurity applicable to organisations in the financial services sector. In the absence of any codified law, the Central Bank of Ireland has published Cross Industry Guidance, which relates to IT governance and risk management by regulated financial institutions in Ireland. The publication makes a number of recommendations including (but not limited to): the preparation of a well-considered and documented strategy to address cyber risk; the implementation of security awareness training programmes; the performance of cyber risk assessments on a regular basis; and the implementation of strong controls by firms over access to their IT systems. Once transposed, the NISD will introduce security measures and Incident reporting obligations for credit institutions. See also reference to Payment Sources Regulations in question 2.1 above.

(b) While there are no specific laws on cybersecurity, electronic communications companies (such as telecoms companies and ISPs) are governed by the DPA, and also the e-Privacy

Regulations. Under the e-Privacy Regulations, there are more explicit rules governing the security of personal data. The electronic communications sector has been further affected by the introduction of the DPA in May 2018. Businesses in the sector have had to familiarise themselves with the new requirements introduced, notably in the areas of transparency, security and accountability for controllers and processors. Certain operators (IXPs, DNS service providers and TLD name registries) will also fall within the ambit of the NISD, upon domestic implementation.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

While there are no express directors' duties specific to cybersecurity, directors owe fiduciary duties to their company under common law and under the Companies Act 2014 (the "**CA 2014**").

There are a number of key fiduciary duties of directors set out in the CA 2014. This list, however, is not exhaustive. Some examples of directors' duties which could be considered to extend to cybersecurity are:

- exercise their powers in good faith in what the director considers to be the interests of the company;
- act honestly and responsibly in relation to the conduct of the affairs of the company;
- act in accordance with the company's constitution and exercise his or her powers only for the purposes allowed by law;
- exercise the care, skill and diligence which would be exercised in the same circumstances by a reasonable person having both the knowledge and experience that may reasonably be expected of a person in the same position as the director with the knowledge and experience which the director has; and
- have regard to the interests of its employees in general.

Directors have a general duty to identify, manage and mitigate risk and fiduciary duties, such as those outlined above, which would extend to cybersecurity. Such duties could be interpreted to mean that directors should have appropriate policies and strategies in place with respect to cyber risk and security and that directors should review and monitor these on a regular basis. Regard may also be had to compliance by a company with all relevant legislative obligations imposed on that company in assessing compliance by directors with their duties. Appropriate insurance coverage should also be considered.

Directors should be fully briefed and aware of all of the key issues relating to cyber risk. Larger organisations may choose to delegate more specific cyber risk issues to a specific risk sub-committee.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

While there are no such express obligations from a company law perspective, general director fiduciary duties, as well as best corporate governance practices, may dictate that such actions are performed. See question 4.1 above for more detail on directors' duties. For industry-specific requirements, see question 3.1 above.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

While there are no such express obligations from a company law perspective, general director fiduciary duties, as well as best corporate governance practices, may dictate that such actions are performed. See question 4.1 above for more detail on directors' duties.

The e-Privacy Regulations oblige electronic communications service providers to report all data breaches to the DPC. The DPA has introduced a more general personal data breach notification obligation to the DPC, which may be of relevance to an Incident. The NISD will introduce Incident reporting obligations for certain operators of essential services.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

This chapter sets out the principal laws and requirements relating to cybersecurity in Ireland. However, there may be other requirements and/or recommendations established by industry-specific codes of conduct. In addition, there may be other laws that do not directly relate to cybersecurity but which establish requirements that bear on cybersecurity. See, in addition, section 2 above.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

As discussed in response to question 5.3 below, an Incident may give rise to various claims under the law of tort. It is also conceivable that an Incident would, depending on the circumstances, give rise to a claim for breach of contract where the particular Incident constituted a breach of contract between the parties.

In order to be entitled to compensation in damages, whether under a tortious or contractual analysis, a plaintiff will be required to establish: that a duty or obligation was owed to him/her by the defendant; that an Incident has occurred in consequence of the defendant's having acted in breach of that duty or obligation; and loss or damage has been sustained to the plaintiff which, but for the impugned acts or omissions of the defendant, would not have been so sustained.

It should be noted that many classes of Incident will also give rise to claims for damages for breach of the constitutional right to privacy. Moreover, where an Incident is committed by a State actor, for example, during the course of an investigation, it may give rise to an action in judicial review to prevent misuse of any inappropriately obtained data and/or to quash any decision taken in relation to, and/or on foot of, the Incident or any improperly obtained data.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Duggan v Commissioner of an Garda Síochána, Ireland and the Attorney General [2017] IEHC 565 – This case affirmed the previously stated position from *Collins v FBD Insurance Plc* [2013] IEHC 137 that a breach of the Data Protection Acts 1988 and 2003 would not automatically entitle a data subject to compensation irrespective of

whether or not they could prove actual loss or damage. The High Court concluded that a data subject has no entitlement to automatic compensation for a technical breach of his/her rights under the Data Protection Acts 1988 and 2003 where he/she cannot prove that he/she has suffered loss or damage as a result of the breach.

CRH plc and Others v Competition and Consumer Protection Commission [2017] IECS 34 – The Supreme Court upheld the finding of the High Court that, in seizing material unrelated to an investigation, the Competition and Consumer Protection Commission had acted outside the scope of its statutory powers and would be acting in breach of the applicants' rights to privacy were it to examine such material. In the exercise by the State of its powers of search, the Supreme Court held that interference with the right to privacy was inevitable but that such interference must be proportionate.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Depending on the specific type of Incident concerned, liability in tort may arise. Examples of such tortious liabilities are as follows:

- The DPA permits a data subject to take a data protection action against a controller or processor where they believe their rights have been infringed. This is deemed to be an action founded in tort. Importantly, the DPA confirms that the damage for which the data subject is seeking compensation need not be just financial. A data subject can sue for other types of damage including pain and suffering.
- A breach of a person's privacy rights may give rise to a claim in tort for breach of confidence or negligence, depending upon the circumstances.
- Incidents involving the theft of information or property may give rise to claims in the tort of conversion.
- Incidents involving the publication of intrusive personal information may in some circumstances constitute the tort of injurious or malicious falsehood.
- Incidents involving the misuse of private commercial information may give rise to claims for damages for tortious interference with economic relations.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

While relatively novel in Ireland, "cyber insurance" products are being taken up by businesses with increasing frequency. Such products afford cover for various data- and privacy-related issues including: the financial consequences of losing or mis-appropriating customer or employee data; the management of a data breach and attendant consequences, including the costs associated with involvement in an investigation by the DPC and fines levied for breaches; and the costs associated with restoring, recollecting or recreating data after an Incident.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no legal limits placed on what the insurance policy can cover. In the ordinary way, however, the consequences of intentional wrongdoing tend to be contractually excluded, as are the consequences of failure to remedy ascertained weaknesses or shortcomings in systems.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

An employer should avoid covert and excessive monitoring of employees. Under the DPA and the ECHR, employees are entitled to privacy, which generally means that employers must balance their need to monitor employees for the purposes of protecting their business against the individual employee's right to privacy. Each case would be decided on its particular circumstances.

The Irish whistleblowing legislation, the Protected Disclosures Act 2014, protects employees from penalisation arising out of reporting actual or possible wrongdoing. In addition, the employer should keep in mind its obligations under data protection legislation when processing personal data, including that such data is kept secure and, where applicable, obligations arising under the e-Privacy Regulations and under the NISD (when implemented). Employees should be made aware, typically by means of a written company policy or relevant provision in the employment contract, of such obligations and their duty to adhere to such obligations on behalf of the company.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No. Whistleblowing laws do not limit or prohibit such reporting by an employee; instead, they are intended to protect the employee from penalisation following his/her making such a report to the employer.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Under the 2017 Act, the Irish police force (generally operating out of the Garda National Economic Crime Bureau) is given a relatively broad authority to investigate cybersecurity Incidents or suspected activity. Specifically, a warrant is obtainable so as to enter and search a premises, and examine and seize (demanding passwords, if necessary) anything believed to be evidence relating to an offence, or potential offence, under the 2017 Act, from a District Court Judge on foot of a suitable Garda statement, on oath.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no requirements under Irish law for organisations to implement backdoors to their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys.

Kevin Harnett
Maples and Calder
75 St. Stephen's Green
Dublin 2
Ireland

Tel: +353 1 619 2036
Email: kevin.harnett@maplesandcalder.com
URL: www.maplesandcalder.com

Kevin joined Maples and Calder in 2009 and was elected as a partner in 2016. He previously worked for a multinational software company as corporate counsel and prior to that, he trained and practised with a large Irish corporate law firm. Kevin has extensive experience advising both domestic and multinational clients on large and complex commercial disputes, including proceedings before the Commercial Court, as well as all forms of alternative dispute resolution and related advisory work. He has a particular focus on the financial services, technology and construction sectors.

Victor Timon
Maples and Calder
75 St. Stephen's Green
Dublin 2
Ireland

Tel: +353 1 619 2071
Email: victor.timon@maplesandcalder.com
URL: www.maplesandcalder.com

Victor is a consultant and head of our Commercial Technology and Privacy group. He has over 35 years' experience in the technology industry. Victor joined Maples and Calder in 2013 and previously worked as in-house counsel in technology firms and as a partner in major law firms in the UK and Ireland. His technology practice includes system procurement, outsourcing, online trading, cloud computing, data protection, privacy and cybersecurity.

MAPLES

Maples and Calder is a leading international law firm advising financial, institutional, business and private clients around the world, on the laws of the British Virgin Islands, the Cayman Islands, Ireland and Jersey.

The firm's affiliated organisation, MaplesFS, provides specialised fiduciary, corporate formation and administrative services to corporate, finance and investment funds entities. The Maples group comprises over 1,700 staff in 16 offices. Since establishing in Ireland in 2006, the Dublin office has grown to over 350 people and has advised on many high-profile and complex transactions in Ireland.

Israel

Haim Ravia

Dotan Hammer

Pearl Cohen Zedek Latzer Baratz

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Section 4 of the Israeli Computers Law, 5755-1995 criminalises unlawful intrusion into computer material. The term "intrusion into computerized material" is defined in the statute as "intrusion by communicating with or connecting to a computer, or by operating it, but excluding intrusion that constitutes wiretapping" under the Israeli Wiretap Law, 5739-1979. This offence carries a maximum penalty of three years' imprisonment.

Section 5 of the Computers Law penalises intrusion into computer material committed in furtherance of another predicate felony. The maximum penalty for this offence is five years' imprisonment.

A 2017 landmark Supreme Court judgment broadly interpreted the boundaries of the term "intrusion into computerized material" to cover any access to a computer absent the owner's permission or some other legal authority. Prosecutions of this offence are becoming more abundant, such as with disgruntled former employees hacking into their former employer's systems, hackers hacking into web-connected cameras, terrorism-oriented hacking and bank account hacking.

Denial-of-service attacks

Denial of service attacks fall within the scope of Section 2 of the Israeli Computers Law, which penalises any obstructions to the ordinary operation of a computer or interference with its use. The maximum penalty for this offence is three years' imprisonment.

Phishing

Phishing falls within the scope of two traditional offences codified in the Israeli Penal Law, 5737-1977, the first being receipt of something by fraud (Section 415 of the Penal Law). This offence is punishable by a maximum term of three years in prison, but if the offence is committed in aggravating circumstances, the maximum punishment is five years in prison. The second offence is receipt of something by ploy or by intentional exploitation of another person's mistake (Section 416 of the Penal Law), punishable by two years' imprisonment. These offences have been the subject of indictments such as online bank account phishing and Facebook account phishing.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Section 6 of the Israeli Computers Law criminalises the programming or adaptation of a computer program for the purpose of unlawfully performing any one of six enumerated acts. Among the enumerated acts is interfering with the ordinary operation of a computer, impacting the integrity of computerised content, facilitating unlawful intrusion into computers or invading a person's privacy. This offence is punishable by up to three years' imprisonment. The act of trafficking in or installing such computer programs is punishable by up to five years in prison. Developers and distributers of spyware, worms, trojans and viruses have been prosecuted under these provisions.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

The installation of software or other tools used to commit cybercrime is an offence under Section 6 of the Israeli Computers Law. This also applies to hardware with a firmware component. While mere possession is likely not an offence, it may amount to an attempt to commit the offence. An attempt is punishable by the same prison term prescribed for the completed offence.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity theft or identity fraud can give rise to two traditional offences codified in the Israeli Penal Law, 5737-1977 – receipt of something by fraud and receipt of something by ploy, both discussed above. In addition, using the identity credentials of another person can give rise to the offence of impersonating another person with intent to defraud, codified in Section 441 of the Israeli Penal Law and punishable by up to three years in prison.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft can give rise to the traditional offence of larceny codified in the Israeli Penal Law, punishable by up to three years in prison, or up to seven years if the stolen property is valued at ILS 500,000 or more. Theft by an employee is a more egregious offence, punishable by up to seven years' imprisonment. If the theft involves data whose confidentiality was compromised by the theft, and the confidentiality arises from an obligation under law, the theft amounts to a criminal invasion of privacy punishable by up to five years' imprisonment.

Copying, importing, renting out or distributing infringing copies of copyrighted material, as well as possession of such copies for the purpose of trafficking are offences under the Israeli Copyright Law, 5768-2007 if they are committed in a commercial scope. These are punishable by up to five years' imprisonment.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Other activities that adversely affect or threaten the security, confidentiality, integrity or availability of any IT system,

infrastructure, communications network, device or data are likely captured by the above offences.

Failure by an organisation to implement cybersecurity measures

Under the Israeli Protection of Privacy Law, 5741-1981, certain organisations are required to appoint an information security officer. Details can be found in the answer to question 4.2 below. Under Section 31A(a)(6) of the Israeli Protection of Privacy Law, failure to appoint an information security officer where such is mandated by the law is a strict lability offence punishable by up to one year in prison.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The above offences have extraterritorial application in three main scenarios. First, if the offence was only partially committed outside Israel, the conduct will be fully captured by the above offences.

Second, if preparations to commit the offence, an attempt to commit it, inducement of another to commit the offence, or conspiracy to commit the offence were performed outside Israel, but the completed offence would have been committed in whole or in part in Israel, then the conduct will be fully captured by the above offences.

Finally, where an offence was committed outside Israel but was targeted against the State of Israel in the broad sense of the phrase (e.g., against national security, the State's regime, the State's property or economy), or was committed by an Israeli resident or citizen, then the conduct will be fully captured by the above offences.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The traditional affirmative defences to criminal culpability also apply to these offences. These defences include necessity, duress and self-defence, yet the bar is rather high to meet. Additionally, both prosecutorial discretion and sentencing guidelines would take into account mitigating factors such as the severity of the conduct, the degree of wilfulness, the scope of harm or affected victims, the motives, etc.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Several other criminal offences which in themselves are not specific to cybersecurity have been used to indict defendants in Israel. Under the specific circumstances of those cases, those charges were applied to cybersecurity matters or to Incidents.

In a recent case, the State of Israel indicted a former employee of an Israeli cyber company in the cyber intelligence business. The defendant was charged with misappropriating intellectual property (cyber and espionage software) and attempting to sell it for $50 million over the Darknet, in a manner potentially harmful to national security. He was also indicted for an *attempt to damage property aimed at impairing national security*, an offence under section 108 of the Penal Law, and for *marketing export-controlled materials without a defence marketing licence*, an offence under section 32 of the Defense Export Control Law, 5767-2007.

In the criminal case of *Israel v. Abu Atza*, the defendant was accused of breaking into a victim's car and stealing her handbag, which contained her smartphone. He allegedly published intimate photos of her which he found on her phone, posting them on her own Instagram account. He was also indicted for *sexual harassment*, an offence under section 3 of the Prevention of Sexual Harassment Law, 5758-1998.

In the case of *Israel v. Oyda*, the defendant, a resident of the Gaza Strip, used software named "Website Hacking" to access the Israeli Police's website and display live streams of traffic cameras in order to gather intelligence against the State of Israel. The defendant had also accessed drone telecommunications for these purposes. He was also indicted with and convicted of *membership and activity in an illegal organisation*, an offence under section 85 of the Defense Regulations, and *espionage*, an offence under section 112 of the Penal Law.

In the case of *Israel v. Massrawa*, the defendant used usernames and passwords he collected through a phishing scam, in order to access victim's bank accounts and transfer funds from those accounts. He was also indicted with and convicted of *money laundering*, an offence under section 3 of the Prohibition on Money Laundering Law, 5760-2000.

In the case of *Israel v. Mualem* (decided on June 30, 2016), the defendant installed monitoring software called "SpyPhone" on personal phones of victims, at the requests of private investigators. The defendant was charged with and convicted of *assisting wiretapping without proper authority*, an offence under section 2 of the Wiretap Law.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Laws applicable to cybersecurity include the Israeli Computers Law, the Protection of Privacy Law, the Penal Law, the Defense Export Control Law, the Regulation of Security in Public Bodies Law, and the recently proposed Cyber Defense and National Cyber Directorate Bill.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The Regulation of Security in Public Bodies Law authorises the Israeli Security Agency and the National Cyber-defense Authority to issue binding directives to organisations operating critical infrastructures on matters related to information security and cybersecurity, and inspect such organisations' compliance with those directives. Organisations subject to this regime include telecom and internet providers, transportation carriers, the Tel Aviv Stock Exchange, the Israeli Internet Association, utility companies and others.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Aside from the cybersecurity requirements applicable to critical infrastructures as explained in the preceding question, the Protection of Privacy Regulations (Data Security), 5777-2017, is an omnibus set of rules. It requires any Israeli organisation that owns, manages or maintains a database containing personal data to implement prescriptive security measures, whose main objective is the prevention of Incidents. These include, for example, physical security measures, access control measures, risk assessment and penetration tests. The regulations classify databases into four categories (basic, intermediate, high and those held by individuals), with each subject to an escalating set of information security requirements.

The regulations also require organisations to monitor and document any event that raises suspicion of compromised data integrity or unauthorised use of data.

Additionally, organisations that hold certain sensitive information are required under the data security regulations to implement an automated audit mechanism to monitor any attempt to access information systems that contain personal data. Sensitive information covers information regarding an individual's private affairs, including: individuals' behaviour in the private domain; health or mental condition; political opinions or religious beliefs; criminal history; telecommunication meta data; biometric data; financial information regarding individuals' assets, debts and economic liabilities; and consumption habits of an individual which may be indicative of the above-mentioned types of data.

In addition, financial institutions and insurance companies are required to operate a security operation centre tasked with monitoring, detecting and mitigating cybersecurity risks.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Use of certain information security measures may constitute telecommunication wiretapping or invasion of privacy. The Israeli Protection of Privacy Law prescribes a number of affirmative defences to invasion of privacy, which are arguably invokable in case of a conflicting legal requirement. Additionally, Section 64 of the proposed Cyber Defense and National Cyber Directorate Bill proposes an exemption from liability for unlawful wiretapping, invasion of privacy, or intrusion into computers, if an organisation takes steps in furtherance of cybersecurity, maintains a cybersecurity policy and is transparent to affected individuals about its use of cybersecurity measures.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There are several provisions according to which certain organisations are required to report Incidents.

First, under the Israeli data security regulations, any organisation that is subject to the intermediate security level or the high security level is required to notify the Protection of Privacy Authority (the Israeli privacy regulator) of the Incident. The notification must state the measures taken to mitigate the Incident.

The intermediate security level applies to public agencies, organisations that hold sensitive information and data brokers. The high security level applies to organisations that hold sensitive information or data brokers, in each case of at least 100,000 data subjects or with more than 100 persons with access credentials.

Second, financial institutions and insurance companies are required to report Incidents pursuant to regulatory guidelines by the Israeli Banking Regulator, and insurance companies are required to report to the Israel's Capital Market, Insurance and Savings Authority within the Ministry of Finance.

There are no formally specified defences or exemptions by which an organisation might prevent publication of information relating to an Incident.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Voluntarily sharing information about an Incident with the Israeli privacy regulator is a permissible practice that the Israeli privacy regulator encourages in the present cybersecurity landscape. If the Incident eventually turns out to be one for which a notification to the regulator was required, the Israeli privacy regulator will tend to view the voluntary early disclosure as a mitigating factor in regulatory action it might take.

Sharing information about an Incident with a foreign authority is the *de facto* result of non-Israeli data breach notification laws with a long reach, such as the GDPR and state data breach laws in the United States.

Finally, sharing information about an Incident with other private sector organisations or trade associations in Israel raises anti-trust issues, but is conditionally permissible pursuant to the Anti-Trust Commissioner's opinion from 2017, if the information shared does not pertain to the business activities of the organisation.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

In certain circumstances, the Israeli privacy regulator may order the organisation after consultation with the Head of the National Cybersecurity Authority, to report the Incident to all affected data subjects. No test case has triggered this to date and thus the particulars of this issue are not yet known.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The data breach notification obligation, as applied by the Israeli data security regulations, depends on the database's security level, which in turn depends on the nature of the information it stores. See the answer to question 2.5 for more information. Yet if the breached data is not capable of identifying an individual, then the Incident need not be reported, since it does not pertain to regulated "personal data".

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Israeli privacy regulator is responsible for enforcing the data security regulations. The Banking Supervisor at the Bank of Israel is responsible for enforcing the data breach rules relating to Incidents in banks and credit card companies. The Supervisor of Capital Markets, Insurance and Savings within the Israeli Ministry of Finance is responsible for enforcing the data breach rules relating to Incidents at insurance companies.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

There are currently no penalties imposable by the Israeli privacy regulator for failing to comply with the data breach notification requirement. A proposed amendment to the Israeli Protection of Privacy Law would empower the regulator with authority to impose penalties.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Recently, the Israeli privacy regulator investigated a data breach revealed in an Israeli company in the business of vehicle location monitoring. The data breach was revealed by an anonymous hacker, who exploited a security vulnerability in the company's website. The regulator launched enforcement action against the company and concluded that it had violated the Israeli data security regulations by not providing a timely notice to the regulator about the Incident.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Among those considered to be investing the most resources in cybersecurity are banks and credit card companies. This is likely due to them operating in a heavily regulated environment with a highly risk-averse regulator. At the other end of the spectrum are many small and medium businesses that often lack the resources for or awareness to, cybersecurity and compliance with the Israeli data security regulations.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Banks and credit card companies are subject to the cybersecurity requirements laid down by the Supervisor of Banks at the Israeli Central Bank. One of the operative requirements for banking corporations and credit card companies is to appoint a cyber-defence manager and define the board of directors' responsibilities in this realm. They are required to continuously examine the effectiveness of the various cyber-defence controls that they have established – using tools such as vulnerability reviews and controlled-intrusion tests.

Insurance companies and investment firms are subject to the cybersecurity requirements laid down by the Supervisor of Capital Markets, Insurance and Savings. They are required, for instance, to approve, at least once a year, a corporate policy on cybersecurity risk management. They must appoint a chief cybersecurity officer and conduct an annual assessment of the suitability of defensive measures to the organisation's overall cybersecurity risks.

The Regulation of Security in Public Bodies Law authorises the Israeli Security Agency and the National Cyber-defense Authority to issue binding directives to telecom organisations operating critical infrastructures on matters related to information security and cybersecurity. These directives are not published.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

There has yet to develop any Israeli case law on the issue of directors' liabilities relating to cybersecurity, and the Israeli Securities Authority has not published any guidelines on the matter. However, cybersecurity guidelines issued by the Supervisor of Banks and the Supervisor of Capital Market, Insurance and Savings do specifically impose duties of oversight on the board of directors of these covered entities. Failure to so do may amount to the directors breaching their duty of care.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Under the Israeli Protection of Privacy Law, certain organisations are required to appoint an information security officer. These organisations include public agencies, service providers who process five or more databases of personal data by commission for other organisations and organisations that are engaged in banking, insurance and credit evaluation.

Organisations that are subject to the Israel data security regulations must establish and maintain procedures for Incident response.

Organisations that are subject to the intermediate or high security levels under the data security regulations are required to perform cyber risk assessments. Organisations that are subject to the high security level are also required to conduct assessments to identify cybersecurity risks.

Any organisation that is subject to the data security regulations is required to oversee and supervise its vendors' data security compliance on an annual basis.

Finally, organisations that are subject to the high level of security are required to perform penetration tests once every 18 months.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

All publicly traded companies are required to include in their periodic reports details of all types of risks that the company is exposed to in light of their line of business, the environment in which they operate and the characteristics unique to their operations. A recent research found that nearly half of the top 125 companies traded on the Tel Aviv Stock Exchange did not report cybersecurity as a risk.

The Israeli Securities Authority has not issued guidelines on the requirement of immediate market disclosure as applied to an Incident. Yet the existing requirements for immediate market disclosures in case of material events are arguably sufficient to capture Incidents that may have a material impact on a reasonable investor in a publicly traded company.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

We are not aware of other requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The most prominent civil action that may be brought against a legal entity in relation to an Incident is class action lawsuit in accordance with the Israeli Class Action Law, 5766-2006.

In order for the court to certify a class action suit, the representative plaintiff must prove that: (1) the action raises substantive questions of fact or in law common to all members of the putative class that were affected by the Incident, and that it is reasonably possible that such questions will be resolved in the class's favour; (2) under the circumstances of the case, a class action is the efficient and fair method to dispose of the dispute; (3) there are reasonable grounds to assume that the interests of all members of the class will be appropriately represented and conducted; and (4) there are reasonable grounds to assume that the interest of all members of the group will be represented and conducted in good faith.

In addition, any person or legal entity that suffered damages related to an Incident may assert a personal civil action based on several applicable laws; for example – invasion of privacy in accordance with the Protection of Privacy Law or for negligence in accordance with the Israeli Torts Ordinance.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

The Incident involving the vehicle monitoring company described in the answer to question 2.11 above has led to at least two class action suits filed against the company, alleging that the company negligently failed to safeguard consumer information.

In September 2017, a similar class action lawsuit was filed against Leumi Card Ltd., an Israeli credit card issuer, following a severe Incident in 2014 where former company employees had stolen vast amounts of information on credit card holders and tried to extort millions of shekels from the company. The class action lawsuit alleges that the company negligently failed to safeguard consumer information.

In April 2011, the Herzliya Magistrate Court awarded ILS 400,000 to a plaintiff for damages he suffered after the defendants infected his personal computer with a Trojan in the wake of a family dispute.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

A person or entity responsible for safeguarding data against an Incident may arguably be liable in tort for failing to take the security measures required under the Israeli data security regulations in negligence or the tort of breach of a legal duty.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents, and it is in fact becoming more common.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no noteworthy regulatory limits.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

Israeli legislation does not specifically address the issue of monitoring and accessing employees' communications and files. This legislative gap has been filled by case law, the most notable being a judgment delivered by the Israeli National Labor Court in 2011, known as the Isakov case. The judgment expounded Israeli privacy law as applied to employers monitoring and accessing employees' communications and files. The decision sets forth the boundaries of permissible access to employee's email communications. The ruling also sets forth a stringent set of pre-requisites and conditions for permissible access.

There are no specific requirements under Applicable Law regarding the reporting of cyber risks or Incidents by employees. Such requirements can be contractually stipulated in an employment agreement. Arguably, they can also be interpreted, in appropriate circumstances, to be part of an employee's general fiduciary obligations towards the employer or part of an employee's duty to act in good faith.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

We are not aware of any such laws.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Israeli Police is empowered with general authority to investigate crimes and to seize documents, objects and computer materials that can potentially serve as evidence relating to the commission of a crime. Seizure of computers and computer material used by a business for investigation purposes requires a court order.

The Israeli privacy regulator has investigative powers relating to violations of the Israeli Protection of Privacy Law, including issues relating to the cybersecurity of databases containing personal data.

The Israeli Wiretap Law authorises investigative and security authorities to surreptitiously obtain the content of real time communications, for national security purposes or for the purpose of preventing and investigating serious crime. Wiretaps sought for preventing and investigating serious crime are subject to court approval, which in exceptional cases can be sought after the fact.

The Israeli Telecom Data Law provides police and various other investigative bodies with the authority to apply to the court of lowest instance in Israel to seek a comprehensive order to surreptitiously receive metadata (but not the content) of telecommunications, for the purpose of search and rescue, investigating or preventing crime, or seizing property. If metadata is required urgently and a court order cannot be obtained in time, such metadata may be obtained for a limited period of 24 hours, without a court order, subject to approval by a senior police officer.

Recently, a proposal for a Cyber Defense and National Cyber Directorate Bill was published. It proposes granting far-reaching and unprecedented powers to the National Cyber Directorate, such as compelling organisations to produce any information or document required to handle cyber-attacks and authority to issue instructions to organisations, including instructions to carry-out acts on the organisation's computerised material, for the purpose of handling cyber-attacks.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Section 11 of the General Security Service Law, 5762-2002 (the statute governing the operation of the Israeli Security Agency, colloquially known as "Shabak" or "Shin Bet"), grants the Prime Minister sweeping powers to order that metadata and non-real time telecommunications be retained by telecom providers and surreptitiously made available to the Shabak.

Section 13 of the Communications Law (Telecommunication and Broadcasts), 5742-1982, provides that the Prime Minister may order telecom service providers to render services to police, security agencies and intelligence agencies, and to have the providers install devices, take measures or adapt their facilities to assist the authorities.

Haim Ravia
Pearl Cohen Zedek Latzer Baratz
Azrieli Sarona Tower
121 Menachem Begin Rd.
Tel-Aviv, 6701203
Israel

Tel: +972 3 303 9058
Fax: +972 3 303 9001
Email: HRavia@PearlCohen.com
URL: www.pearlcohen.com
www.law.co.il

Haim is a Senior Partner and Chair of the Internet, Cyber and Copyright Practice Group at Pearl Cohen Zedek Latzer Baratz. Haim deals extensively with data protection and privacy, cyber & internet law, IT contracts, copyright, electronic signatures, and open source software. Haim was a member of the Israeli public commission for the Protection of Privacy, and was part of a governmental team that re-examined the Israeli law pertaining to personal information databases. Haim received an acknowledgment award from the Israel Chamber of Information System Analysts for pioneering and innovation in the Israeli internet. Practising internet and cyber law for over 20 years, Haim has also written numerous columns on internet law for *Globes* (a major Israeli financial newspaper), the *Israel Bar Association Magazine* and other publications. Haim also operates Israel's first legal website (www.law.co.il) and publishes commentaries on *Lexology*.

Dotan Hammer
Pearl Cohen Zedek Latzer Baratz
Azrieli Sarona Tower
121 Menachem Begin Rd.
Tel-Aviv, 6701203
Israel

Tel: +972 3 303 9037
Fax: +972 3 303 9001
Email: DHammer@PearlCohen.com
URL: www.pearlcohen.com
www.law.co.il

Dotan is a Senior Associate and member of the Internet, Cyber and Copyright Group at Pearl Cohen Zedek Latzer Baratz. Dotan regularly advises on Israeli data protection and privacy laws. Having completed his academic degree in computer science at the age of 19, later working as a software developer and a technological project leader, Dotan also counsels clients on the privacy and data protections aspects of software and SaaS user agreements and licensing, as well as on other IT law matters such as digital (electronic) signatures, copyright issues and open source matters. Dotan regularly contributes to Israel's first legal website (www.law.co.il), *Lexology* and other online publications.

PEARL COHEN

Pearl Cohen Zedek Latzer Baratz ("Pearl Cohen") is an international law firm with offices in Israel, the United States and the United Kingdom, offering legal services across numerous practice areas.

Pearl Cohen's Data Protection and Privacy Practice Group in Israel comprises seasoned attorneys who leverage their nuanced understanding of new technologies and their experience in internet and cyber law to offer clients comprehensive legal services for the growing complexities of information and data privacy regulations.

At times, data protection and privacy matters entail court or administrative proceedings. Pearl Cohen's Data Protection and Privacy Practice Group has accumulated vast experience in representing clients before the Israeli Protection of Privacy Authority, and before Israeli courts in privacy and data protection litigation.

Italy

Giuseppe Vaciago

Marco Tullio Giordano

LT42 – The Legal Tech Company

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Unauthorised access to a computer or telecommunications system (Article 615 *ter*, Code of Criminal Law). This crime requires a person to obtain access to a protected information or telecommunications system against the express or implied consent of the individual entitled to exclude third parties from gaining such access. The punishment is imprisonment for up to three years.

Digital fraud or *fraud* (Article 640 *ter*, Code of Criminal Law). This crime occurs when whoever – knowingly and with intent to defraud – tampers with one or more digital devices, unlawfully using information, data or software on a digital device, in order to gain money and harm someone else. The punishment is imprisonment for between six months and three years.

Fake identity (Article 494, Code of Criminal Law). The article at hand is applicable to real identities as well as digital identities; the relevant crime is perpetrated when someone falsely and wilfully represents himself or herself to be someone else. The punishment is imprisonment for up to one year.

Illegal possession and diffusion of passwords to digital systems (Article 615 *quater*, Code of Criminal Law). This crime is perpetrated when a person unlawfully has or spreads secret access codes, in order to gain money or harm someone else. The punishment is imprisonment for up to one year.

Denial-of-service attacks

Damage of digital information, data or software (Article 635 *bis*, Code of Criminal Law). This occurs when someone intentionally damages, destroys, deletes or disables any kind of digital information, data or software belonging to someone else. The punishment is imprisonment for between six months and three years.

Phishing

Digital fraud or fraud (Article 640, Code of Criminal Law) – *see above.*

Fake identity (Article 494, Code of Criminal Law) – *see above.*

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Unauthorised access to a computer or telecommunications system (Article 615 *ter*, Code of Criminal Law) – *see above.*

Damage of digital information, data or software (Article 635 *bis*, Code of Criminal Law) – *see above.*

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Illegal possession and diffusion of passwords to digital systems (Article 615 *quater*, Code of Criminal Law) – *see above.*

Identity theft or identity fraud (e.g. in connection with access devices)

Digital fraud or fraud (Article 640 or 640 *ter*, Code of Criminal Law) – *see above.*

Fake identity (Article 494, Code of Criminal Law) – *see above.*

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Unlawful disclosure of secret professional information (Article 622, Code of Criminal Law). This crime requires an individual to purposefully disclose to any other persons any kind of secret information that she or he knows because of her/his profession or job. The punishment is imprisonment for up to one year.

Unauthorised access to a computer or telecommunications system (Article 615 *ter*, Code of Criminal Law) – *see above.*

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Unlawful interception and destruction of communications (Article 616, Code of Criminal Law). This crime is perpetrated when a person opens, steals or destroys correspondence, including emails, not addressed to him or her. The punishment is imprisonment for up to one year.

Unlawful interception, distortion, falsification, destruction of communications (from Article 617 *bis* to 617 *sexies*, Code of Criminal Law). These different offences, punished through several articles, occur when a person opens, steals or destroys correspondence, including emails, not addressed to him or her, even with software, malware or any kind of digital tools having one of those purposes. The punishment is imprisonment for between six months/one year and four years.

Unlawful disclosure of mails (Article 618, Code of Criminal Code). This crime is perpetrated when a person intentionally discloses, or endeavours to disclose, to any other person, the contents of any wire, verbal, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, verbal, or electronic communication in breach of this provision. The punishment is imprisonment for up to six months.

Failure by an organisation to implement cybersecurity measures

From Article 167 to Article 172 of the Data Protection Code – as amended and supplemented by the European General Data Protection Regulation (GDPR) – criminal penalties, such as imprisonment from six months to six years, are expressly provided in case of:

- unlawful data processing (where breaches pertain to, for example, information notice, consent, sensitive data, traffic data, location data, unsolicited communications and so on);
- untrue statements and notifications submitted to the Italian Personal Data Protection Authority;
- failure to comply with the security measures set out by the Data Protection Code; and
- failure to comply with regulations issued by the Italian Personal Data Protection Authority and other mandatory obligations pertaining to employees' personal data protection.

Furthermore, the Data Protection Code expressly states that being convicted of any of the offences above shall always entail publication of the relevant judgment.

1.2 Do any of the above-mentioned offences have extraterritorial application?

All the offences mentioned at in the answer to question 1.1 have extraterritorial application if the victim is an Italian citizen or if the criminal conduct has been at least partially taken place in the Italian territory (Article 6 of the Code of Criminal Law).

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

When the Applicable Law is the NIS Directive/Decree No. 65/2018, there is a mitigation (a ⅓ reduction of the penalty) in case there are security measures put in place. According to the GDPR, there are also some mitigations in case of compliance with security standards.

Furthermore, Law No. 48/2008, which ratified the 2001 Budapest Convention on Cybercrime, updated both the Data Protection Code and Legislative Decree No. 231/2001 and introduced corporate criminal liability in connection with cyber and computer crimes committed in the interest of the company. However, companies may shield themselves from liability arising from the commission of crimes if, among other things, prior to the crime's commission, they adopt and effectively implement a compliance model designed to prevent crimes of the same kind as the one committed.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

In the Italian jurisdiction, a draft act has been proposed; if it is passed, legal hacking by police in case of investigations of suspects of the most serious crimes like terrorism and mafia activity shall be allowed.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Over the last 20 years, Italy has been developing a new framework of laws (which are often driven by international regulations and other countries' experiences) on cybersecurity matters.

Below is a brief summary of each regulation:

- Italian Criminal Law: as mentioned above, cybersecurity is also taken into account in Legislative Decree No. 231/2001 and Law No. 48/2008, which introduced corporate criminal liability in connection with cyber and computer crimes perpetrated in the interest of the company.
- GDPR and Italian implementation (Legislative Decree No. 101/2018): also known as the General Data Protection Regulation, European Regulation 2016/679 concerns the protection of individuals with regard to the processing of personal data and the free movement of such data. The Italian implementing legislation of GDPR (Legislative Decree No. 101/2018) shall be enforceable from 21 November 2018.
- NIS Directive and implementing Legislative Decree No. 65/2018: the most recent development is European Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 *concerning measures for a high common level of security of network and information systems across the Union*. Finally, the recent Government Decree of 18 May 2018 implemented Directive 1148/2016/EU.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The Italian legislation implementing the NIS Directive is Legislative Decree No. 65/2018, which was approved on 16 May 2018 but is only enforceable from 24 June 2018.

Like the Directive, the Decree promotes risk management activities and specific duties of reporting of security Incidents in the main critical infrastructure sectors and introduces standards and measures in order to improve the national cybersecurity system.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Regarding such measures, Article 14 NIS Directive and Article 32 GDPR have several features in common.

Article 14 NIS Directive, as well as the Article 14 Paragraph 1 of the implementing Legislative Decree No. 65/2018 (with exactly the same wording) states that operators of critical infrastructure take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information

systems which they use in their operations. With regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

Article 32 GDPR – Security of Processing requires all organisations to ensure a level of security appropriate to the risk, taking appropriate technical and organisational measures, which include ongoing confidentiality, integrity, availability and resilience of IT systems, the capacity to restore the availability of and access to IT systems in the event of a physical or technical Incident, regular testing, assessment and evaluation of the measures to manage and secure IT systems.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

There are some issues regarding the former regulatory framework and the new framework of laws.

1) There are several notifications required to be made for a single IT Incident or data breach to different authorities according to the following list of European regulations that are applicable in Italy:
   - notification of data breaches – Article 33 GDPR, which states that companies must notify data breaches to the Italian Data Protection Authority and to individuals when such breaches affect the rights and freedoms of personal data subjects involved in a breach;
   - notification of data breaches – Articles 14–16 NIS Directive and Articles 12–14 Legislative Decree No. 65/2018, which state that companies must notify data breaches to the Computer Security Incident Response Team (CSIRT), the Data Protection Authority and individuals when such breaches affect the rights and freedoms of personal data subjects involved in a breach;
   - Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; and
   - Circular No. 285 of 17 December 2013, which mandates a notification to the Bank of Italy and the European Central Bank in case of data breaches in the Italian banking sector.
2) According to the GDPR and the NIS Directive, organisations could potentially be fined twice, because the relevant requirements overlap in many places, which has inevitably led to several questions that judges will have to deal with.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

The circumstances in which this reporting obligation is triggered are as follows:

a) Data breach according to the GDPR.
b) IT Incident according to Legislative Decree No. 65/2018.
c) IT Incident according to Bank of Italy regulations (Circular No. 285 of 17 December 2013).
d) IT Incident of digital signature according to Regulation (EU) No. 910/2014.

The regulatory or other authorities to which the information is required to be reported are as follows:

a) GDPR: within 72 hours to the Data Protection Authority.
b) Legislative Decree No. 65/2018: as soon as possible to the Italian CSIRT.
c) Circular No. 285 of 17 December 2013: as soon as possible to Bank of Italy.
d) Regulation (EU) No. 910/2014: within 24 hours to AgID (Agency for Digital Italy).

The nature and scope of information that is required to be reported are as follows:

a) GDPR: categories of involved data, measures taken before the Incident and recovery plan.
b) Legislative Decree No. 65/2018: type of Incident, measures taken before the Incident and recovery plan.
c) Circular No. 285 of 17 December 2013: type of Incident and recovery plan.
d) Regulation (EU) No. 910/2014: type of Incident and recovery plan.

The exemptions by which the organisation might prevent publication of that information are as follows:

a) GDPR: personal data unintelligible to any person who is not authorised to access it, as in encryption.
b) Legislative Decree No. 65/2018: none.
c) Circular No. 285 of 17 December 2013: none.
d) Regulation (EU) No. 910/2014: none.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Article 18 Legislative Decree No. 65/2018 (voluntary notification) provides that any company, even if is not listed as a critical infrastructure operator, can notify the competent authority of any breach which may a significant impact on the continuity of its services.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

As mentioned at question 2.4, currently several regulations provide for notifications to be made to data subjects in case of IT Incidents. The Applicable Laws are the following:

- Notification of data breaches as well as Article 34 GDPR, Articles 14–16 NIS Directive and Articles 12–14 Legislative Decree No. 65/2018 provide for companies to notify individuals of IT Incidents when such Incidents affect the rights and freedoms of personal data subjects who are involved in the breach.

- Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, repealing Directive 1999/93/EC.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The responses to questions 2.5 and 2.7 do not change if the information includes the listed items.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Italian Data Protection Authority (*Garante per la protezione dei dati personali*), is an independent administrative authority set up by the so-called Privacy Law (Law No. 675 of 31 December 1996) and subsequently regulated by the Data Protection Code.

Article 7 of the implementing Legislative Decree provides a list of Italian ministries designated for each sector, regulated by Article 8 NIS Directive:

a) the Ministry of Economic Development for the energy sector;
b) the Ministry of Infrastructure and Transport for infrastructure;
c) the Ministry of Economics and Finance for the bank sector and stock exchanges;
d) the Ministry of Health for the healthcare sector; and
e) the Ministry of Environment for the environmental sector.

All ministries are in charge of controlling, monitoring and regulating the implementing legislation and keeping this innovative regulation updated.

Furthermore, according to Legislative Decree No. 65/2018, the Italian Presidency of the Council of Ministers is implementing the CSIRT.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

- In case of a lack of implementation of appropriate technical and organisational measures to ensure a level of security which is adequate for the risk (Article 32 GDPR) or missed notification of a data breach (Article 33 GDPR), a company can be subject to administrative fines of up to 10,000,000 EUR, or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- According to Legislative Decree No. 65/0218, in case of omitted measures, a company can be fined in the range of 12,000 to 120,000 EUR. In case of an omitted notification of an IT Incident to the Italian CSIRT, a company can be fined in the range of 25,000 to 125,000 EUR.
- Electronic Identification, Authentication and Trust Services (eIDAS): an omitted notification to the AgID and violations of the provisions can be fined by the Authority in the range of 40,000 to 400,000 EUR according to Article 32 *bis* of the Digital Administration Code (also known as CAD).
- Circular 285/2013: for omitted notifications to the Bank of Italy it is provided that an Italian bank can be fined from 2,400 to 129,210 EUR according to Article 144 of the Consolidated Law on Banking (also known as TUB).

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

It must be noted that on 11 May 2017, even before the application of the European Regulations, an Italian Telecommunication Company (Wind Tre S.p.A.) was fined by the Italian Data Protection Authority for having breached its duty of notification to individuals affected by a personal data breach.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The financial services and telecommunications sectors are focused on IT security more than others. In fact, there are authorities entrusted with specific oversight in some areas, e.g.: IVASS – the Institute for the Supervision of Insurance Companies; Bank of Italy – which supervises banks and non-banking intermediaries entered in specific registers; and AGCOM – the communications authority.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

As previously mentioned, the NIS Directive was implemented into Italian legislation by Legislative Decree no. 65/2018, which is the main law focused on these two specific sectors.

For the financial services sector, in particular focusing on Italian banks, reference can be made to Circular No. 285 of 17 December 2013, which provides a notification to the Bank of Italy and the European Central Bank in case of data breaches in the Italian banking sector.

For insurance companies, Regulation No. 38 of 3 July 2018 of IVASS provides specific cybersecurity measures for Italian insurance companies.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

According to the GDPR and the NIS Directive, *accountability* is the main principle that the liability of a company is based on and then, if necessary, responsibilities of managers and directors would be scrutinised in relation to their duties, in case of lack of measures and cyber-resilience. Under Italian corporate law, company directors are required to manage the company in compliance with the duties imposed on them both by law and by the company's articles of association. Pursuant to Article 2392 of the Civil Code, the members of the board of directors of a stock company are jointly liable to the company for damage arising from the breach of duties imposed on them either by the law or by the company's articles of association.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) No, there is no requirement about designating a CISO.

(b/c/d) According to the GDPR, NIS Directive and Legislative Decree No. 65/2018, in Italy, companies must have policies and conduct risk assessments and penetration test/vulnerability assessments in order to be compliant with Article 32 GDPR which provides implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Differently, according to the NIS Directive there is a duty to cooperate nationally in case of an Incident, which means that companies in both sectors must implement a policy to respond correctly.

As aforementioned, Legislative Decree No. 65/2018 does not provide for any additional rules in this case.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Legislative Decree No. 101/2018 recalls Articles 33 and 34 of the GDPR, which require data controllers to report personal data breaches to a supervisory authority without undue delay and, where feasible, within 72 hours of breach discovery. Additionally, data controllers must also communicate to the affected EU citizens if there is a high risk that the breach will affect their rights and freedoms.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

In Italy, there are several secondary laws and regulations which improve the implementation of IT security measures in some businesses. Certainly, the financial sector is one of the most focused on cybersecurity, because nowadays all financial transactions are digitalised. For reference, please see, e.g.:

- Circular No. 285 of 17 December 2013, in relation to the Italian banking sector.
- Regulation No. 38 of 3 July 2018 of IVASS (Institute for the Supervision of Insurance Companies).

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

All things considered above, it is also important to understand how the Italian legal system defines data processing and what can happen in case of judiciary cases for omitted cybersecurity measures.

With regard to the protection of personal data, data processing is considered to be a "dangerous activity" subject to Article 2050 of the Italian Civil Code. This provision is generally significant, but especially in this case because it reverses the burden of proof and provides that the damaged party has the right to be indemnified by the entity that carried out the data processing if that entity is not able to demonstrate that it took all the necessary measures to avoid the damage.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

The Italian Protection Authority has already provided for telecommunications companies (2013) and public administrations (2015) the obligation of notification of data breaches to the Authority. Currently, all of them are under the European legislation (NIS Directive and GDPR). In particular, on 16 May 2018 a case was decided for the most important Italian telecommunication company (Tim S.p.A.), which was fined 960,000 EUR for two different violations: 1) for having unlawfully processed personal data of a client, who was registered with 826 mobile phone numbers; and 2) for having been affected by a data breach which in 2013 caused the disclosure of personal data of some clients on web accounts of other clients.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

One of the key concepts of the innovative legislative framework of the European privacy law is accountability. The fundament of this responsibility is that companies should be compliant with some general principles stated by the GDPR and NIS Directive (Legislative Decree No. 65/2018).

One of those principles concerns the duty of companies to take organisational measures that must ensure a level of security adequate to the risk posed in every specific core business (Article 32 GDPR and Article 14 Legislative Decree No. 65/2018). Management must also prevent and minimise the impact of Incidents that affect systems so that the continuity of services is not affected.

In case of cyber Incidents, companies – in order to exclude their liability – should be in a position to provide sound evidence they have prepared and enforced policies/procedures and security practices as part of their compliance process.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, any company is allowed to take out insurance against cyber Incidents. As expected, new privacy regulations have been a catalyst for accelerated growth of cyber-insurance in the European market, where demand has been always incomparable to the US market, which is the largest. As well as in the rest of Europe, the Italian cyber-insurance trend is growing rapidly, but it is not increasing enough compared to the United States.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

The most important regulatory limitation is that cyber-insurance cannot cover penalties imposed by the law.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The surveillance and other monitoring tools of employees are subject to the application of Article 4 of Law no. 300/1970, implemented by Legislative Decree 151/2015.

Article 4 of the Italian Workers' Statute of Rights (Law no. 300/1970) prevented the use of any technical or mechanical control over employees' activity until September 2015, when the Italian Jobs Act introduced some significant changes. On one side the approach of Article 4 has been confirmed, and the use of instruments and equipment which are specifically aimed at controlling employees is still prohibited. Similarly, the new rules confirmed that those instruments and equipment which are potentially able to remotely monitor employees are allowed only to the extent they are required to satisfy organisational, production-related or security needs, and provided that their use is agreed upon with the Trade Unions or authorised by the Labour Inspectorate.

Moreover on 1 March 2007, the Italian Data Protection Authority issued the Guidelines for the use of email and internet services where some important rules are established in order to regulate the data processing by the company. In particular, it has been confirmed that the employer has the power to control data processing to the extent that:

- a dangerous situation – even a potential one – cannot be prevented through prior technical interventions;
- the control is of the overall consolidated data processed by a business unit or a particular office (i.e.: administration, sales, finance and the like);
- the control is concluded by issuing a general warning in the event that an abnormal use is detected; and
- the control is not prolonged for an undetermined time. Regarding this principle, on 1 February 2018 the Data Protection Authority, which was handling a compliant of an employee, fined a company for having kept emails of employees with no specific purpose.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

Law No. 179/2017, which is enforceable from 29 December 2017, expands existing whistleblowing protections to the private sector, requiring companies that have adopted formal compliance programmes pursuant to the mentioned Legislative Decree No. 231/2001 (corporate liability) to also implement a formal whistleblower programme. Specifically, the policy must provide for:

- more than one whistleblowing channel able to protect whistleblowers' identities, of which at least one has to be computerised;
- the prohibition of acts of discrimination or retaliation against whistleblowers;
- disciplinary measures for those who retaliate against a whistleblower and for the whistleblowers who intentionally or with gross negligence file false or unsubstantiated reports of violations; and
- the confidentiality of a whistleblower's identity to the extent permitted by Italian law.

There is no specific prohibition about IT security reports, but obligations of notifying and reporting must find a balance with requirements provided by Legislative Decree No. 179/2017.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Data Protection Authority inspection powers are laid out in Section 158 of Legislative Decree No. 196/2003. When investigating organisations, the Authority can request information and documents, although these requests are not legally binding. However, if there is no cooperation, and the organisation refuses access to its systems, the Authority can apply for a judicial order to carry out an investigation, even with the involvement of the tax police (Italian law enforcement officer competent for data protection). When carrying out formal inspections, the Data Protection Authority can demand copies of records and databases, which may be passed onto the judicial authorities. A report of the outcome is then published.

- The Bank of Italy supervises banks and non-banking intermediaries entered in specific registers. Since November 2014, this supervision has been conducted within the framework of several pieces of legislation, even secondary legislation provided directly by the Bank of Italy, which means even enforcement issues regarding the Circular No. 285 of 2013.
- IVASS – the Institute for the Supervision of Insurance – is an authority under public law whose goal is to ensure adequate protection of insured persons with a view to the sound and prudent management of insurance and reinsurance undertakings and their transparency and fairness towards customers. This means that one of the tasks of IVASS is the enforcement of cybersecurity and data protection for Italian insurance companies.
- Furthermore, the Italian Criminal Law allows prosecutors to investigate with the police and army, which means that in force of several kinds of judiciary acts, companies must give certain required information, including: price-sensitive information; IP addresses; email addresses; and personally identifiable information of cyber threat actors, and of individuals who have been inadvertently involved in an Incident. This means that in case of criminal cases (which are listed in section 1), authorities can conduct thorough investigations.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, in the Italian jurisdiction there is no Disclosure Law, and one of the basic principles of the Italian Criminal Law is the privilege against self-incrimination and the presumption of innocence.

Giuseppe Vaciago
LT42 – The Legal Tech Company
Via Vitruvio 1
20124 Milano
Italy

Tel: *+39 02 211 150*
Email: *g.vaciago@lt42.it*
URL: *www.lt42.it*

Giuseppe Vaciago has been a lawyer of the Milan Bar since 2002, is Of Counsel at R&P Legal Firm and founder of LT42. For the last 10 years, his primary focus has been IT law and cybercrime. He has assisted many national and international IT companies. Academically, he received his Ph.D. on Digital Forensics from Università di Milano and he is a Professor at Insubria University (Varese and Como), where he teaches a course on IT law. He attended Fordham Law School and Stanford Law School as a Visiting Scholar to expand his studies in his own particular research area. Giuseppe Vaciago is the author of many publications on cybercrime, including both scientific journals and textbooks, which have been adopted by the university where he teaches. He is fellow at the Cybercrime Institute of Koln and a member of the Editorial Board of the *Journal of Digital Investigation*.

Marco Tullio Giordano
LT42 – The Legal Tech Company
Via Vitruvio 1
20124 Milano
Italy

Tel: *+39 02 211 150*
Email: *m.giordano@lt42.it*
URL: *www.lt42.it*

Qualifying as an attorney-at-law in 2008, Marco Tullio Giordano has built up considerable experience in criminal law relating to new technology, with a particular focus on cybersecurity, privacy-related crimes and ISP liability. He is also a certified ISO/IEC 27001:2014 lead auditor. He is a senior associate of R&P Legal Firm and co-founder of LT42. He works as outside counsel for a number of leading web companies, managing law enforcement liaison and privacy and data protection issues. As a criminal lawyer, he provided assistance in court to private individuals and companies in several computer-related criminal cases. The author of a number of publications concerning cybercrime and privacy issues, he also contributes online, writing articles and comments on the law and new technology.

LT42 is an Italian Legal Tech Company. Our main challenge is to transform legal services into automated processes. Our main focuses are compliance and cybersecurity. LT42 was founded through a project to create a network of highly skilled professionals who are willing to innovate in the legal sector by joining not only legal and technical skills but also risk management, communication and digital reputation management. The ultimate goal is to become an integrated one-stop-shop for the legal professionals.

Differently from many other "tech-legal" companies, LT42 always provides a hi-tech service with top-notch legal skill.

Japan

Mori Hamada & Matsumoto

Hiromi Hayashi

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

As background, there are two main laws criminalising cyber attacks, namely (A) the Act on the Prohibition of Unauthorized Computer Access (the "**UCAL**"), and (B) the Penal Code.

(A) The UCAL imposes criminal sanctions on any person who makes an Unauthorized Access to a computer (an "**Access Controlled Computer**"), the access to and operation of which are under the control of an administrator (the "**Access Administrator**").

An "**Unauthorized Access**" means any action which operates an Access Controlled Computer by either (i) inputting an identification code (*shikibetsu-fugou*) (e.g., password and ID) allocated to a user who is authorised to access the Access Controlled Computer (an "**Authorized User**"), without the permission of the Access Administrator or the Authorized User, or (ii) inputting any information (other than an identification code) or command which enables that person to evade control (e.g., cyber attack of a security flaw), without the permission of the Access Administrator (UCAL, Article 2, Paragraph 4).

The UCAL prohibits the following actions:

(a) an Unauthorized Access (Article 3);

(b) obtaining the identification code of an Authorized User to make an Unauthorized Access (Article 4);

(c) providing the identification code of an Authorized User to a third party other than the Access Administrator or the Authorized User (Article 5);

(d) keeping the identification code of an Authorized User which was obtained illegally to make an Unauthorized Access (Article 6); and

(e) committing the following acts by impersonating the Access Administrator or causing a false impression of being the Access Administrator: (a) setting up a website where the fake Access Administrator requests an Authorized User to input his/her identification code; or (b) sending an email where the fake Access Administrator requests an Authorized User to input his/her identification code (Article 7).

Any person who commits (a) above (Article 3) is subject to imprisonment of up to three years or a fine of up to JPY 1,000,000 (Article 11). Any person who commits (b) to (e) above (Articles 4 to 7) is subject to imprisonment of up to one year or a fine of up to JPY 500,000 (Article 12). However, if the person committing (c) (Article 5) does not know that the recipient intends to use the identification code for an Unauthorized Access, that person is subject to a fine of up to JPY 300,000 (Article 13).

(B) The Penal Code provides for criminal sanctions on the creation and provision of Improper Command Records which give improper commands, such as a computer virus, to a computer (*fusei shirei denji-teki kiroku*). "**Improper Command Records**" means (i) electromagnetic records that give a computer an improper command which causes the computer to be operated against the operator's intention or to fail to be operated in accordance with the operator's intention, and (ii) electromagnetic or other records which describe such improper commands.

Under the Penal Code, any person who creates or provides, without any justifiable reason, Improper Command Records or who knowingly infects or attempts to infect a computer with Improper Command Records is subject to imprisonment of up to three years or a fine of up to JPY 500,000 (Article 168-2). Any person who obtains or keeps Improper Command Records for the purpose of implementing such records is subject to imprisonment of up to two years or a fine of up to JPY 300,000 (Article 168-3).

In addition, the Penal Code provides for the following additional penalties:

(i) any person who obstructs the business of another by causing a computer used in the business to be operated against the operator's intention, or to fail to be operated in accordance with the operator's intention, by (a) damaging that computer or any electromagnetic record used by that computer, or (b) giving false information or an improper command to the computer, is subject to imprisonment of up to five years or a fine of up to JPY 1,000,000 (Article 234-2);

(ii) any person who gains or attempts to gain, or causes or attempts to cause a third party to gain, illegal financial benefits by (a) creating false electromagnetic records by giving false information or an improper command to a computer, or (b) providing false electromagnetic records, for processing by a third party, in either case in connection with a gain, a loss or a change regarding financial benefits, is subject to imprisonment of up to 10 years (Article 246-2); and

(iii) any person who creates, provides or attempts to provide electromagnetic records for the purpose of causing a third party to mistakenly administer matters which relate to rights, obligations or proofs of facts, is subject to imprisonment of up to five years or a fine of up to JPY 500,000. However, if the act relates to records to be made by public authorities or public servants, the penalty is imprisonment of up to 10 years or a fine of up to JPY 1,000,000 (Article 161-2).

Hacking (i.e. unauthorised access)

Hacking is an Unauthorized Access under the UCAL, punishable by imprisonment of up to three years or a fine of up to JPY 1,000,000.

If the hacking is made through Improper Command Records, it is also punishable under the Penal Code (please see question 1.1(B) above). In addition, if a business is obstructed by such hacking, the crime is punishable by imprisonment of up to five years or a fine of up to JPY 1,000,000 (Penal Code, Article 234-2).

Denial-of-service attacks

This carries the same penalties as hacking.

Phishing

Article 7 of the UCAL prohibits phishing, while Article 4 of the UCAL prohibits obtaining any identification code through phishing. These actions are punishable by imprisonment of up to one year or a fine of up to JPY 500,000 (Article 12).

In addition, any person who gains illegal benefits by using identification codes obtained by phishing is subject to imprisonment of up to 10 years under Article 246-2 of the Penal Code.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

This carries the same penalties as hacking.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Any person who obtains or keeps Improper Command Records for the purpose of using such records is subject to imprisonment of up to two years or a fine of up to JPY 300,000 (Penal Code, Article 168-3).

As an example, nine persons were prosecuted for uploading software which contained a computer virus to an online storage system and which infected the computers of people who accessed the storage and downloaded the software from September to December 2016.

Identity theft or identity fraud (e.g. in connection with access devices)

This carries the same penalties as phishing.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

In addition to the criminal penalties applicable to phishing, electronic theft is penalised under the Unfair Competition Prevention Act. If a current or former employee (a) acquires a trade secret of the employer through theft, fraud, threat, or other illegal actions (the "**Illegal Actions**"), including an Unauthorized Access, or (b) uses or discloses a trade secret of the employer acquired through Illegal Actions, for the purpose of obtaining wrongful benefits or damaging the owner of the trade secret, that employee is subject to imprisonment of up to 10 years or a fine of up to JPY 20,000,000, or both (Article 21, Paragraph 1). In addition, if that employee commits any of the foregoing acts outside Japan, the fine is increased up to JPY 30,000,000 (Article 21, Paragraph 3).

Under the Copyright Act, any person who uploads electronic data of movies or music, without the permission of the copyright owner, to enable another person to download them, is subject to imprisonment of up to 10 years or a fine of up to JPY 10,000,000, or both (Article 119, Paragraph 1). Further, any person who downloads electronic data which is protected by another person's copyright, and who knows of such protection, is subject to imprisonment of up to two years or a fine of up to JPY 2,000,000, or both (Article 119, Paragraph 3). In addition, any person who sells, lends, manufactures, imports, holds or uploads any device or program which may remove, disable or change technology intended to protect copyright (e.g., copy protection code), is subject to imprisonment of up to three years or a fine of up to JPY 3,000,000, or both (Article 120-2).

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

This carries the same penalties as electronic theft.

Failure by an organisation to implement cybersecurity measures

The UCAL requires Access Administrators to make efforts to manage the identification codes of Authorized Users, examine the validity of functions to control access to the Access Controlled Computer, and to implement necessary measures, including enhancing functions (e.g., encryption of codes, definite deletion of codes which have not been used for a long time, implementing a batch program to address a security hole, program updates, and appointing an officer for network security) (Article 8). However, there is no criminal sanction on a breach of these obligations.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The UCAL provides for the extraterritorial application of Articles 3, 4, 5 (except where the offender did not know the recipient's purpose) and 6 of the UCAL (Article 14).

The Penal Code has extraterritorial application (Article 4-2).

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

No, there are no such actions.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

No. The Organized Crime Act, which applies to an act of terrorism, designates certain material crimes, such as murder, identified in the Penal Code, and imposes penalties which are heavier than those under the Penal Code. However, criminal offences regarding cybersecurity which are described in question 1.1 above are not designated crimes under the Organized Crime Act.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

In addition to the UCAL, the Penal Code and the Unfair Competition Prevention Act described above, the following laws are also applicable to cybersecurity.

- Basic Act on Cybersecurity

  This provides the basic framework for the responsibilities and policies of the national and local governments to enhance cybersecurity. Further, it obligates operators of

material infrastructure (e.g., financial institutions, operators of railroads, airplanes and other means of transportation, and providers of electricity, gas and water) and networks (e.g., telecommunications networks) to make efforts to voluntarily and proactively enhance cybersecurity and to cooperate with the national and local governments to promote measures to enhance cybersecurity. Based on this Basic Act, the National Center of Incident Readiness and Strategy for Cybersecurity was established in 2015.

A bill to revise the Basic Act in order to establish a cybersecurity council was recently submitted to the Diet. The cybersecurity council is intended to be the avenue which will allow national and local governmental authorities and business operators to share information which may facilitate the proposal and implementation of cybersecurity measures. However, the bill was not approved at the Diet session which took place on July 22 and will be discussed at the next Diet session.

- Telecommunication Business Act (the "**TBA**")

Article 4 of the TBA provides that (1) the secrecy of communications being handled by a telecommunications carrier shall not be violated, and (2) any person who is engaged in a telecommunications business shall not disclose secrets obtained, while in office, with respect to communications being handled by the telecommunications carrier, even after he/she has left office.

The secrecy of communications protects not only the contents of communications but also any information that would enable someone to infer the meaning or the contents of communications. In this regard, data on access logs and IP addresses are protected under the secrecy of communications. If a telecommunications carrier intentionally obtains any information protected under the secrecy of communications, discloses protected information to third parties, and uses protected information without the consent of the parties who communicated with each other, that telecommunications carrier is in breach of Article 4(1).

To prevent cyber attacks, it would be useful for telecommunications carriers to collect and use information regarding cyber attacks, e.g., access logs of infected devices, and share information with other telecommunications carriers or public authorities. However, the TBA does not explicitly provide how a telecoms carrier may deal with cyber attacks without breaching Article 4(1). The Ministry of Internal Affairs and Communications ("**MIC**"), the governmental agency primarily responsible for implementing the TBA, issued reports in 2014 and 2015 which address whether a telecoms carrier may deal with cyber attacks and the issues that may arise in connection with the secrecy of communications. The findings in both reports are included in the guidelines on cyber attacks and the secrecy of communications (the "**Guidelines**") issued by the Council regarding the Stable Use of the Internet (the "**Council**"), a council composed of five associations which include the Japan Internet Providers Association, a voluntary association of telecommunications carriers, cable TV service providers and other companies conducting businesses related to the Internet. The Guidelines include the contents of MIC's 2014 and 2015 reports. The Guidelines, however, are not legally binding, although they carry a lot of weight because MIC confirmed them before they were issued by the Council.

Further, in 2013, MIC started a project called ACTIVE (Advanced Cyber Threats response InitiatiVE) that aims to protect Internet users from cyber attacks by collaborating with ISPs and vendors of IT systems. To prevent computer virus infections, warning users or blocking communications in accordance with the Guidelines may be done by ISPs which are members of ACTIVE. For example, according to ACTIVE's release dated February 26, 2016, MIC has started a program through ACTIVE to prevent malware infection. The program aims to mitigate damage by blocking telecommunications between the malware and the C&C (Command and Control) server and by warning users who have infected devices. According to the website of ACTIVE, ACTIVE gathers information from business operators such as vendors of IT systems and makes a list of computer viruses and malware and infected websites.

In addition, in May 2018, the TBA was amended to introduce a new mechanism which enables a telecommunications carrier to share with other carriers information on transmission sources of cyber attacks. The amendments will be effective in November 2018.

- Act on the Protection of Personal Information (the "**APPI**")

The APPI is the principal data protection legislation in Japan. It is the APPI's basic principle that the cautious handling of Personal Information under the principle of respect for individuals will promote the proper handling of Personal Information. "**Personal Information**" means information about specific living individuals which can identify them by name, date of birth or other descriptions contained in the information (including information that will allow easy reference to other information which may enable individual identification) (Article 2, Paragraph 1). A business operator handling Personal Information may not disclose or provide Personal Information without obtaining the subject's consent, unless certain conditions are met.

To prevent cyber attacks, it would be useful for business operators to collect and use information regarding the cyber attacks, e.g., access logs of infected devices, and share information with other business operators or public authorities. However, if the information includes Personal Information, it would be subject to the restrictions on the use and disclosure of Personal Information under the APPI.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The UCAL requires Access Administrators to make efforts to manage the identification codes of Authorized Users, examine the validity of functions to control access to the Access Controlled Computer, and implement necessary measures, including enhancing functions (e.g., encryption of codes, definite deletion of codes which have not been used for a long time, implementing a batch program to address a security flaw, program updates, and appointing an officer for network security) (Article 8).

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The Ministry of Economy, Trade and Industry ("**METI**") and the Independent Administrative Agency Information-technology Promotion Agency ("**IPA**") jointly issued the Cybersecurity Management Guidelines (the latest version of which is as of November 2017). The guidelines describe three principles that the management of companies, which have a dedicated division for information system and are utilising IT, should recognise to protect their company from cyber attacks and 10 material items on which

management should give instructions to executives or directors in charge of IT security including the chief information security officer ("**CISO**").

The 10 material items and some examples of recommended actions for each item described in the guidelines are as follows:

(i) Recognise cybersecurity risks and develop company-wide measures

Example: Develop security policy which incorporates cybersecurity risk management while aligning it with the company's management policy so that management can publish company-wide measures.

(ii) Build a structure or process for cybersecurity risk management

Example: CISO to establish a system to manage cybersecurity risks and set forth the responsibility clearly.

Example: Directors to examine whether a system which will manage cybersecurity risks has been established and is being operated properly.

(iii) Secure resources (e.g., budget and manpower) to execute cybersecurity measures

Example: Allocating resources to implement specific cybersecurity measures.

(iv) Understand possible cybersecurity risks and develop plans to deal with such risks

Example: During a business strategy exercise, identify information which needs protection and cybersecurity risks against the information (e.g., damage from leakage of trade secrets on a strategic basis).

(v) Build a structure to deal with cybersecurity risks (i.e., structure to detect, analyse and defend against cybersecurity risks)

Example: Secure the computing environment and network structure used for important operations by defending them at multiple layers.

(vi) Publish cybersecurity measures framework ("**PDCA**") and its action plan

Example: Develop a structure or process where one can constantly respond to cybersecurity risks (assurance of implementation of PDCA).

(vii) Develop an emergency response system (emergency contacts, initial action manual, and Computer Security Incident Response Team ("**CSIRT**")), and execute regular hands-on drills

Example: Issue instructions to promptly cooperate with relevant organisations and to investigate relevant logs to ensure that efficient actions or investigations can be taken to identify the cause and damage of a cyber attack.

Example: Execute drills, including planning activities, to prevent recurrence after Incidents and reporting Incidents to relevant authorities.

(viii) Develop a system to recover from the damages caused by an Incident

Example: Establish protocols for recovery from business suspension or other damages caused by an Incident and execute drills in accordance with protocols.

(ix) Ensure that entities in the company's entire supply chain, including business partners and outsourcing companies for system operations, take security measures

Example: Conclude agreements or other documents to provide clearly how group companies, business partners and outsourcing companies for system operations in the company's supply chain will take security measures.

Example: Have access to and understand reports on how group companies, business partners and outsourcing companies for system operations in the company's supply chain take security measures.

(x) Collect information on cyber attacks through participation in information-sharing activities, and develop the environment to utilise such information

Example: Help society guard against cyber attacks by actively giving, sharing and utilising relevant information.

Example: Report information on malware and illegal access to the IPA in accordance with public notification procedures (standards for countermeasures for computer viruses and for illegal access to a computer).

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

The secrecy of communications is strongly protected under the TBA. To prevent cyber attacks, it would be useful for telecommunications carriers to collect and use information regarding the cyber attacks, e.g., access logs of infected devices, and share information with other telecommunications carriers or public authorities. However, the TBA does not explicitly provide how a telecoms carrier may deal with cyber attacks without breaching Article 4(1). Thus, it is difficult for telecommunications carriers to balance prevention of cyber attacks with the protection of secrecy of communications. MIC tried to deal with this issue by helping to establish the Guidelines, by collaborating with ISPs through ACTIVE and by introducing a new mechanism to share the information on transmission sources of cyber attacks (please see question 2.1 above).

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There is no mandatory requirement to report Incidents.

However, under the guidelines for banks issued by the Financial Services Agency ("**FSA**"), banks are required to report an Incident immediately after becoming aware of it. The guidelines are not legally binding; however, because FSA is a powerful regulator of the financial sector, banks would typically comply with FSA's guidelines (please see question 3.1). The report must include:

(i) the date and time when the Incident occurred and the location where the Incident occurred;

(ii) a summary of the Incident and which services were affected by the Incident;

(iii) causes of the Incident;

(iv) a summary of the facilities affected by the Incident;

(v) a summary of damages caused by the Incident, and how and when the situation was remedied or will be remedied;

(vi) any effect to other business providers;

(vii) how banks responded to enquiries from users and how they notified users, public authorities and the public; and

(viii) possible measures to prevent similar Incidents from happening.

In addition, if a cyber attack causes a serious Incident specified in the TBA and the enforcement rules of the TBA, such as a temporary suspension of telecommunications services or a violation of the secrecy of communications, the telecommunications carrier is required to report the Incident to MIC promptly after its occurrence. In addition, the carrier is required to report the details of the said Incident to MIC within 30 days from its occurrence. The detailed report must include:

(i) the date and time when the Incident occurred;

(ii) the date and time when the situation was remedied;

(iii) the location where the Incident occurred (the location of the facilities);

(iv) a summary of the Incident and which services were affected by the Incident;

(v) a summary of the facilities affected by the Incident;

(vi) details of the events or indications of the Incident, the number of users affected, and the affected service area;

(vii) measures taken to deal with the Incident, including the persons who dealt with it, in chronological order;

(viii) causes which made the Incident serious, including how the facilities have been managed and maintained;

(ix) possible measures to prevent similar Incidents from happening;

(x) how the telecoms carrier responded to inquiries from users and how it notified users of the Incident;

(xi) internal rules in connection with the Incident;

(xii) if the telecoms carrier experienced similar Incidents in the past, a summary of the past Incidents;

(xiii) the name of the manager of the telecoms facilities; and

(xiv) the name and qualifications of the chief engineer of the telecoms facilities.

Further, it is recommended that companies report the Incident to the IPA (please see question 2.3 above). The report must include:

(i) the location where the infection was found;

(ii) the name of the computer virus. If the name is unknown, features of the virus found in the IT system;

(iii) the date when the infection was found;

(iv) the types of OS used and how the IT system is connected (e.g. LAN);

(v) how the infection was found;

(vi) possible cause of the infection (e.g., email or downloading files);

(vii) extent of the damage (e.g., the number of infected PCs); and

(viii) whether the infection has been completely removed.

The IPA also has a contact person whom the companies may consult, whether or not they file a report with the IPA, as to how they can deal with cyber attacks or any Unauthorized Access. According to the IPA's website, it had 7,600 consultations in 2017.

If the Incidents involve any disclosure, loss, or damage of Personal Information handled by a business operator, then, according to the guidelines issued by the Personal Information Protection Committee (the "**PPC**") regarding the APPI, the operator is expected to promptly submit to the PPC a summary of such disclosure, loss or damage, and planned measures to prevent future occurrences.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Please see question 2.5. Further, through ACTIVE, business operators are permitted to share information regarding cyber attacks (please see question 2.1).

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The Cybersecurity Management Guidelines recommend knowing who should be notified if a cyber attack has caused any damage, gathering information to be disclosed, and promptly publishing the Incident, taking into account its impact on stakeholders (please see question 2.3).

Further, if the Incidents involve any disclosure, loss or damage of Personal Information handled by a business operator, then, according to the guidelines issued by the PPC regarding the APPI, the operator is expected, depending on the contents or extent of the disclosure, loss or damage, to notify the affected individuals of the facts relevant to the disclosure, loss or damage, or to make the notification readily accessible to the affected individuals (e.g., posting the notification on the operator's website), in order to prevent secondary damages or similar Incidents.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The secrecy of communications protects not only the contents of communications but also any information that would enable someone to infer the meaning or the contents of communications. In this regard, IP addresses and email addresses are protected under the secrecy of communications. Further, personally identifiable information is protected under the secrecy of communications if it is delivered through telecommunications facilities. With respect to an Incident, a telecommunications carrier may not share information protected under the secrecy of communications unless it complies with the Guidelines or the instructions of ACTIVE (please see questions 2.1 and 2.5).

In addition, personally identifiable information of cyber threat-makers and individuals who have been inadvertently involved in an Incident would be Personal Information under the APPI which cannot be provided to a third party without obtaining the prior consent of the data subjects, except in limited instances. One such exception is where a public authority needs the cooperation of a private person to implement the authority's legal duties, and the performance of those legal duties will likely be impeded if the private person has to

first obtain the data subject's consent. In this regard, the provision of personally identifiable information of cyber threat-makers would not require their consent.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

MIC is the governmental agency primarily responsible for implementing the TBA.

METI is not a regulator that has a specific mandated regulatory authority under specific laws. Rather, it promulgates desirable policies for each industry.

The PPC is an independent organ which supervises the enforcement and application of the APPI.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Other than the report of a serious Incident under the TBA (please see question 2.5), reporting is not mandatory. If a telecommunications carrier does not report a serious Incident, it is subject to a fine of up to JPY 300,000.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

No examples can be found based on publicly available information.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

In general, the financial business sector and the telecommunications service sector closely collaborate with relevant authorities on information security.

In July 2015, FSA issued a summary of its policies to strengthen cybersecurity in the financial business sector. According to the summary, FSA's five policies are: (i) continuous dialogue with financial institutions to understand their cybersecurity risks; (ii) improving information-sharing among financial institutions; (iii) implementing cybersecurity exercises in which financial institutions, FSA and other public authorities participate; (iv) developing cybersecurity human resources; and (v) establishing a department in FSA to handle cybersecurity matters. Based on these policies, FSA amended its guidelines for banks to include standards on cybersecurity management, such as establishing an organisation to handle emergencies (e.g., CSIRT), designating a manager in charge of cybersecurity, preparing multi-layered defences against cyber attacks and implementing a periodic assessment of cybersecurity. The guidelines are not legally binding; however, because FSA is a powerful regulator of the financial sector, banks would typically comply with FSA's guidelines.

As described above, telecommunications carriers are required to report a serious Incident specified in the TBA (please see question 2.5). In addition, if a telecommunications carrier does not take appropriate measures to remedy problems with its services, MIC may order it to improve its business. Failure to comply with the order is subject to a fine of up to JPY 2,000,000.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Please see question 3.1.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Under the Companies Act, a director has the duty to act with "due care as a prudent manager" in performing his/her functions as director (*zenkan chuui gimu*). The applicable standard of care is that which a person in the same position and situation would reasonably be expected to observe. In general, if a director fails to get relevant information, enquire or consider how to prevent Incidents, to the extent these acts are reasonably expected of him/her based on the facts when he/she made a decision (e.g., decision to purchase the IT system), then he/she would be in breach of this duty.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The Cybersecurity Management Guidelines jointly issued by METI and IPA recommend companies to build a structure or process for cybersecurity risk management and, as an example, to designate a CISO according to the companies' policies, including the security policy (please see question 2.3).

Further, FSA's guidelines for banks provide the standards regarding cybersecurity management, such as establishing an organisation to handle emergencies (e.g., CSIRT), designating a manager in charge of cybersecurity and implementing a periodic assessment of cybersecurity (please see question 3.1).

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no disclosure requirements that are specific to cybersecurity risks or Incidents.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, there are no other specific requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Basically, if a person breaches a contract, the other party may bring a civil action based on the breach. The plaintiff has the burden of proving the breach, the damages incurred by it, and the causation between the breach and the plaintiff's damages.

In addition, the Civil Act of Japan provides for a claim based on tort. If a person causes damages to another, the injured party may bring a civil action based on tort. The plaintiff has the burden of proving the damages incurred by it, the act attributable to the defendant, and the causation between the defendant's act and the plaintiff's damages.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

A vendor of a computer system was sued by a company which used the system provided by the vendor. The case related to cyber attacks (SQL injections) to the system which resulted in the disclosure of credit card information of the company's clients. The company sought the payment of damages caused by the cyber attacks in the amount of approximately JPY 100,000,000, based on breach of contract. The Tokyo District Court decided that although the vendor was required to provide programs which are suitable for blocking SQL injections in accordance with existing standards when the computer system was provided, the Incident was also partially attributable to the company because it ignored the vendor's proposal to improve the system. The vendor was ordered to pay only approximately JPY 20,000,000 (Tokyo District Court decision dated January 23, 2014).

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Tort theory is available under the Civil Act of Japan (please see question 5.1).

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. In general, there are two categories of insurance against Incidents, namely (i) insurance to cover the losses incurred by the vendor of an IT system, and (ii) insurance to cover the losses incurred by a business operator using the IT system.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations on insurance coverage under the law. The coverage may differ depending on the insurance products of insurance companies.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

No, there are no specific requirements.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No, there are no Applicable Laws.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcers have the power to investigate Incidents which are related to crimes under Applicable Laws. In accordance with the "cybercrime project" of the National Police Agency, the police in each prefecture have established a contact point where consultations and information regarding cybercrimes are handled.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, there are no such requirements.

Hiromi Hayashi
Mori Hamada & Matsumoto
Marunouchi Park Building, 2-6-1
Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: *+81 3 5220 1811*
Email: *hiromi.hayashi@mhmjapan.com*
URL: *www.mhmjapan.com*

Hiromi Hayashi is a partner at Mori Hamada & Matsumoto, which she joined in 2001. She specialises in communications law and regulation, and authored the Japanese portion of *Telecommunication in Asia* in 2005. Her other areas of practice are international and domestic transactions, takeover bids and corporate restructuring. She was admitted to the Bar in 2001 in Japan and in 2007 in New York. She worked at Mizuho Corporate Bank from 1989 to 1994 and at Davis Polk & Wardwell in New York from 2006 to 2007.

MORI HAMADA & MATSUMOTO

Mori Hamada & Matsumoto is a full-service international law firm based in Tokyo, with offices in Fukuoka, Nagoya, Osaka, Beijing, Shanghai, Singapore, Yangon Bangkok and Ho Chi Minh, and a Jakarta desk. The firm has over 450 attorneys and a support staff of approximately 450, including legal assistants, translators and secretaries. The firm is one of the largest law firms in Japan and is particularly well-known in the areas of mergers and acquisitions, finance, litigation, insolvency, telecommunications, broadcasting and intellectual property, as well as domestic litigation, bankruptcy, restructuring and multi-jurisdictional litigation and arbitration. The firm regularly advises on some of the largest and most prominent cross-border transactions representing both Japanese and foreign clients. In particular, the firm has extensive practice in, exposure to and expertise on, telecommunications, broadcasting, the Internet, information technology and related areas, and provides legal advice and other legal services regarding the corporate, regulatory, financing and transactional requirements of clients in these areas.

Kenya

Hazel Okoth

Stella Ojango

Gikera & Vadgama Advocates

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

The offence of unauthorised access is committed where a person, whether temporarily or permanently, causes a computer system to perform a function by infringing security measures with intent to gain access without authorisation. Access is unauthorised if that person is not entitled to control access of the computer system in question or does not have consent from the person authorised to access the computer system. This offence is punishable by a fine not exceeding Kshs. 5,000,000.00 or to imprisonment for a term not exceeding three years, or both. However, if the unauthorised access is gained with the intent to commit a further offence, the liability on conviction is a fine not exceeding Kshs. 10,000,000.00 or imprisonment for a term not exceeding 10 years, or both.

Denial-of-service attacks

Any person who without lawful authority or lawful excuse does an act which causes a denial of access to any program or data stored in a computer system is liable upon conviction to a fine not exceeding Kshs. 200,000.00 or to imprisonment for a term not exceeding two years, or both.

Phishing

Phishing is described as creating or operating a website or sending a message through a computer system with the intention to induce the user of a website or the recipient of the message to disclose personal information for an unlawful purpose or to gain unauthorised access to a computer system. The liability on conviction is a fine not exceeding Kshs. 300,000.00 or to imprisonment for a term not exceeding three years, or both.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

See below.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

A person who knowingly manufactures, adapts, sells, procures for use, imports, offers to supply, distributes or otherwise makes available a device, program, computer password, access code or similar data designed or adapted primarily for the purpose of committing an offence is liable on conviction to a fine not exceeding Kshs. 20,000,000.00 or to imprisonment for a term not exceeding 10 years, or both.

If a person knowingly receives or is in possession of a program or a computer password, device, access code or similar data procured through any means described above and intends that it be used to commit or assist in the commission of an offence is liable on conviction to a fine not exceeding Kshs. 10,000,000.00 or to imprisonment for a term not exceeding five years, or both.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity theft and impersonation occurs when a person fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person. This offence is punishable by a fine not exceeding Kshs. 200,000.00 or to imprisonment for a term not exceeding three years, or both.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

The general punishment for stealing anything that is capable of being stolen is imprisonment for three years, unless the circumstances of the theft or the nature of the thing stolen dictates some other punishment.

Breach of confidence by an employee does not constitute a criminal offence, but civil proceedings may be instituted against said employee for breach of contract.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Unauthorised disclosure of password or access code – Knowingly and without authority disclosing any password, access code or other means of gaining access to any program or data held in any computer system. This offence is punishable by a fine not exceeding Kshs. 5,000,000.00 or to imprisonment for a term not exceeding three years, or both.

Failure by an organisation to implement cybersecurity measures

The requirement to implement cybersecurity measures is highest on owners of critical information infrastructure as well as organisations in certain regulated industries. The National Computer and Cybercrimes Co-ordination Committee is tasked with regulating the minimum physical and technical security measures that must be implemented in order to protect critical information infrastructure.

The standard of compliance is therefore high but non-implementation nonetheless does not constitute a criminal offence.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The Computer Misuse and Cybercrimes Act does provide for international cooperation in addition to the provisions of our Mutual Legal Assistance Act of 2011 and the Extradition (Contiguous and Foreign Countries) Act. The Office of the Attorney General and the Department of Justice may make a request in any criminal matter to a requested state for purposes of undertaking investigations or proceedings concerning offences related to computer systems, collecting evidence of an offence or obtaining expeditious preservation and disclosure of traffic data or real time collection of traffic data. A requesting state may also make a similar request to the Office of the Attorney General and the Department of Justice, which may either be granted or refused. In any case, any act or omission committed outside Kenya which would, if committed in Kenya, constitute an offence is deemed to have been committed in Kenya if the person committing the act or omission is a citizen of Kenya or ordinarily resident in Kenya and the act or omission is committed against a citizen of Kenya, against property belonging to the Government of Kenya outside Kenya, or to compel the Government of Kenya to do or refrain from doing any act, or if the person who commits the act or omission is after its commission or omission present in Kenya.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Whereas the Computer Misuse and Cybercrimes Act does not specifically provide any actions that may mitigate the penalty of an offence or an exception to any offence, the Kenya Criminal Procedure Code provides that a court may before passing sentence or making any order against an accused person, receive such evidence as it thinks fit in order to inform itself as to the sentence or order to be passed or made. Mitigation is a well-established practice of the Kenyan Courts and some of the factors that the court may consider include the cause of the crime, the magnitude of the crime, prevalence and type of crime, aggravating or extenuating circumstances, the circumstances of the accused, any previous convictions as well the uniformity in the approach to sentencing.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

According to the Kenya Prevention of Terrorism Act, No. 30 of 2012, a terrorist act involves among other things the interference with an electronic system resulting in the disruption of the provision of communication, financial, transport or other essential services. A person who commits a terrorist act that results in this Incident or any other Incident elucidated in the Act is liable to imprisonment for a term not exceeding 30 years and if such an act results in the death of another person, such person is liable to life imprisonment.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Over and above the Computer Misuse and Cybercrimes Act*, the Kenya Information and Communications Act is the substantive law with respect to Data Protection in Kenya.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The Director to the Secretariat of the National Computer and Cybercrimes Co-ordination Committee is responsible for designating a system as critical infrastructure. Within a reasonable time after such declaration of an information infrastructure as critical, the Director shall issue directives to regulate:

- the classification of data held by the critical information structure;
- the protection, storage and archiving of data held by the critical information infrastructure;
- cybersecurity Incident management by the critical information infrastructure;
- disaster contingency and recovery measures which must be put in place by the critical information infrastructure;
- minimum physical and technical security measures that must be implemented in order to protect the critical information infrastructure; and
- the period within which the owner or person in control of a critical information infrastructure must comply with the directives.

The Committee, together with the owner of the critical information infrastructure shall conduct an assessment of the threats and vulnerabilities of a cyber-attack across all critical infrastructure sectors, determine the harm to the economy that would result from damage or unauthorised access to critical infrastructure, measure the overall preparedness of each sector against damage or unauthorised access to critical infrastructure and identify any other risk-based security factors appropriate and necessary to protect public health and safety.

The owner of a critical information infrastructure is required to report to the Committee any Incidents likely to constitute a threat in the nature of an attack that amounts to a cybercrime.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Generally, body corporates shall run their affairs in a manner where the commission of any offence, including a cybercrime, is prohibited

in line with the relevant law. This is done by maintaining various policies such as a cybersecurity policy and general data protection regulations.

Organisations in certain regulated industries, for instance the banking industry, are indeed required to maintain a cybersecurity policy in a manner specified by the regulator as well as to adopt other practices to prevent cyber threats and related Incidents.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Conflicts of laws usually do not arise because any cybersecurity guidelines issued in a specific industry stipulate that such guidelines supplement existing legislation and regulations and in case of any conflict the law will prevail.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

The owner or operator of a critical information infrastructure is required to report to the National Computer and Cybercrimes Co-ordination Committee any Incident likely to constitute a threat in the nature of an attack that amounts to a computer and cybercrime. Moreover, a person who operates a computer system, whether public or private, shall immediately inform the Committee of any attacks, intrusions and other disruptions to the functioning of a computer system or network within 24 hours of such attack, intrusion or disruption. This report shall include information about the breach, including information on how the breach occurred, an estimate of the number of people affected by the breach, an assessment of the risk of harm to the affected individuals and an explanation of any circumstances that would delay or prevent the affected persons from being informed of the breach. The Committee may then propose the isolation of any computer system or network suspected to have been attacked or disrupted pending the resolution of the issues.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

This is not applicable in Kenya.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The report of any cyber threat, intrusion or disruption to the Committee shall include an explanation of any circumstances that would delay or prevent the affected persons from being informed of the breach. Organisations therefore have a duty to report any Incidents or potential Incidents to the affected individuals or otherwise proffer an explanation as to why the affected persons cannot be informed.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Any person or body corporate may provide a reasonable explanation for non-disclosure of sensitive or proprietary information if such information falls within the disclosure requirements of an Incident report to the Committee. In any case, the spirit of the Act is to enable the timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes and not to facilitate the disclosure of confidential information.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Over and above receiving and acting on reports of computer and cybercrimes, the National Computer and Cybercrimes Coordination Committee is responsible for advising the Government on security-related aspects on blockchain technology matters, advising the National Security Council on computer and cybercrimes, co-ordinating national security organs in matters relating to computer and cybercrimes, co-ordination, collection and analysis of cyber threats and response to cyber Incidents that threaten cyberspace belonging to Kenya and establishing codes of cybersecurity practice and standards of performance for implementation by owners of critical national information infrastructure.

It reports to the Cabinet Secretary responsible for matters relating to internal security and regulates its own procedure.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Any person who fails to report a cyber threat is liable upon conviction of a fine not exceeding Kshs. 200,000.00 or imprisonment for a term not exceeding two years or both.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

There are no examples of such enforcement action in Kenya.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

In the financial services sector, the Central Bank of Kenya, which is the regulator of banks, financial institutions and mortgage finance companies, has formulated a Guidance Note on Cyber Security applicable to all institutions licensed under the Banking Act, Chapter 488 of the Laws of Kenya. This Guidance Note sets the minimum standards that institutions must comply with as part of their regulatory obligations and is supplemental to the legislation, regulations and guidelines already in place. It specifically provides for the additional responsibilities of the Board of Directors in relation to cyber risk, senior management responsibility to implement the institution's business strategy, risk appetite and threats, the introduction of the role of the Chief Information Security Officer (CISO), regular independent assessment and testing at least once a year, mitigating the risks of outsourcing services such as cloud providers and providing IT security awareness training programmes for all employees.

The Guidance Note also provides additional reporting requirements for institutions within 24 hours of Incidents that could have a significant adverse impact on the institution's ability to provide adequate services to its customers.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The Computer Misuse and Cybercrimes Act contains requirements that are specific to organisations in the financial services sector as well as the telecommunications sector.

For instance, electronic mail or processes through which money or information is being conveyed must not be intercepted or destroyed and electronic messages must be directed to the rightful recipient.

Various acts, such as sending electronic messages which materially misrepresent any fact upon which reliance by another person will cause that person to suffer any damage or loss, as well manipulating a computer or other electronic payment device with the intent to underpay or overpay, are prohibited by the Act.

The Act further prohibits a person authorised to use a computer or other electronic device for financial transactions, issuance of electronic instructions as they relate to sending of electronic debit and credit messages or confirmation of electronic fund transfer from issuing false electronic instructions.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

The Principal Officer of a body corporate is required to exercise all reasonable care, skill and diligence when carrying out their duties to prevent the commission of an Incident or any cyber-related crime. In addition to the body corporate being found liable for any offence in the nature of a cybercrime, the Principal Officer or anyone acting in a similar capacity will also be deemed to have committed the offence unless they prove that they exercised their fiduciary duty of care.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The Guidance Note on Cybersecurity issued by the Central Bank of Kenya makes all the above recommendations the minimum requirements that institutions licensed under the Banking Act should build upon in the development and implementation of strategies, policies and procedures aimed at mitigating cyber risk.

As part of their cybersecurity policies, organisations have established a unique framework to prevent and indeed mitigate cyber-related risks, which include organisational risk assessment, cybersecurity Incident management, organisation-wide information security awareness and training and regular audits and assessments.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

The reporting requirements of any operator of a computer system, whether public or private, only require the entity to disclose information about the breach and knowledge on how the breach occurred, an estimate of the number of people affected, an assessment of the risk of harm to the affected individuals and an explanation of any circumstances that would delay or prevent the affected persons from being informed of the breach. Service providers, whether public or private institutions, that provide users of its services the means to communicate by use of a computer system or any other entity that processes or stores computer data on behalf of that entity or its users shall not be liable for the disclosure of any data that the service provider discloses to the extent required by the Act.

Listing authorities will specify their disclosure requirements. The contents of a company's annual report will be governed by its articles of association and any other recommendations of the Board. In regulated sectors, however, such as companies in the insurance or banking sector, the regulatory body may specify certain information to be disclosed in the company's annual report.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

This is not applicable in Kenya.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Service providers are liable to both criminal and civil liability if it is established that the service provider had actual notice, actual knowledge, or wilful and malicious intent, and not merely through

omission or failure to act, had thereby facilitated, aided or abetted the use by any person of any computer system controlled or managed by the service provider in connection with the contravention of cybersecurity-related laws.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

There are no examples of such cases in Kenya.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

A potential liability in tort may arise if a complainant is able to demonstrate that an act was committed intentionally against another person with the aim of causing harm or where the offender fails to demonstrate the kind of care a prudent person would take in the same situation and an injury results from any action or inaction.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Cyber Liability Insurance is among the most recent insurance policies available to small and medium-size enterprises as well as large corporations. The policy varies from one insurance provider to another but will typically protect businesses from internet-based risks by mitigating losses relating to damage or loss of information from information technology infrastructure and activities.

As data continues to assert itself as an organisation's most valuable asset, many firms are taking out these types of policies to mitigate the vulnerability of this asset.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Whereas the Insurance Act provides for the framework of insurance policies, no limitations are provided as the risks an insurer can take or mitigate with respect to Cyber Liability Insurance. The insurance policy will vary among the various providers. A first party insurance policy, for instance, will typically cover damage to digital assets, business interruptions, cyber extortion through ransomware and reputational harm, whereas a third-party insurance policy will typically cover liability of cost of forensic investigations, customer notifications, legal defence and regulatory fines.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The law recognises the importance of developing a framework for training employees on the prevention, detection and mitigation of computer and cybercrimes and matters connected thereto. It is also important that cybersecurity awareness and information be provided to customers, clients, suppliers, partners and outsourced service providers.

Whereas the reporting requirements under the Act refer to reporting to the Committee after the occurrence of an Incident, employees owe their employers a reasonable duty of care in the performance of their duties and this would include reporting a potential threat or a security flaw likely to lead to the interception of company data.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

The Kenya Access to Information Act, No. 31 of 2016, protects persons making disclosure of information which the person obtained in confidence in the course of employment; for example, if the disclosure is of public interest. Such disclosure may include information on violations of the law.

In the event that there exists any statutory prohibition or restriction on the disclosure of information, it shall be a defence to show that in the circumstances the disclosure was in the public interest and where the offence is alleged to have been committed by a public officer or Government contractor.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The investigatory powers and procedures with respect to cybercrimes and other criminal offences committed by means of a computer system are exercisable by a police officer, an officer in a law enforcement agency or a cybersecurity expert designated by the Cabinet Secretary responsible for matters relating to national security.

Where any of the aforementioned persons has reasonable grounds to believe that a specified computer system or data is reasonably required for the purpose of criminal investigation or has been acquired by a person as a result of the commission of an offence, the authorised person may apply to court for the issuance of a warrant to enter any premises to search and seize such data.

An authorised person may also apply to court for a production order where they have reasonable ground to believe that specified data are in the control of a person or are in the possession of a service provider.

Where there is risk or vulnerability that data may be modified, lost, destroyed or rendered inaccessible, a police officer or any other authorised person has the power to serve a notice on the person who is in possession or control of the computer system requiring the person to undertake expeditious preservation of such data and disclose such data to identify the service provider and that path through which the communication was transmitted.

Subject to making an application to the court and being awarded the relevant order, authorised persons may also collect real-time traffic data, compel a service provider to record data or to co-operate and assist the competent authorities in the collection or recording of data.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Organisations are not required to implement backdoor systems for law enforcement authorities. Authorised persons must adhere to the provisions of the law with respect to accessing any computer system or data and will procure a court order where applicable to access any such system or information.

Note

* The constitutionality of the Computer Misuse and Cybercrimes Act, No. 5 of 2018, is currently been challenged at the Constitution and Human Rights Division of the Kenyan High Court and certain provisions therein have been suspended. The matter is coming up for ruling on 3rd October 2018.

The Act has only recently come into force, and, as of the time of writing, no proceedings have yet been determined under this law.

This chapter is up to date as of 21st September 2018.

Hazel Okoth
Gikera & Vadgama Advocates
56 Muthithi Road
Behind TRV Office Plaza
Westlands, P.O. Box 720-00621
Nairobi
Kenya

Tel: +254 721 112 167
Email: hokoth@gvalawfirm.com
URL: www.gvalawfirm.com

Hazel Okoth is an Associate at the Head Office in Nairobi and specialises in Commercial, Trade and Intellectual Property matters at the Firm. She holds a degree from the University of Nairobi and a Postgraduate Diploma from the Kenya School of Law. She also holds a Higher Diploma from the Institute of Human Resource Management and is a member of the Project Management Institute as well as the Anti-Counterfeiting Committee of the International Trademark Association (INTA). Hazel has been a delegate and has spoken on various trade-related aspects at the Kenya Trade Week organised by the Ministry of Trade.

In addition to her knowledge on cybersecurity, she has advised on the protection of intellectual property rights in various jurisdictions and undertakes due diligence, investigations and drafts agreements relating to confidentiality, non-solicitation, licences and assignments.

Stella Ojango
Gikera & Vadgama Advocates
56 Muthithi Road
Behind TRV Office Plaza
Westlands, P.O. Box 720-00621
Nairobi
Kenya

Tel: +254 723 755 243
Email: sojango@gvalawfirm.com
URL: www.gvalawfirm.com

Mrs Stella Ojango is an Advocate of the High Court of Kenya, with over six years' experience as a legal practitioner and is a Partner with the Firm. Stella holds a Bachelor of Laws degree from Moi University, Kenya, and a Postgraduate Diploma in Law from Kenya School of Law. She is currently undertaking her Master's degree in Environmental Law at the University of Nairobi.

Stella has a distinguished track record of delivering valuable advice on real estate projects, from property acquisition, to obtaining the requisite approvals, securing development financing, preparing the requisite contract documents, registration and handover of developments. She is adept at advising institutions on risk management, corporate governance and legal compliance. She has expertise in legislative drafting, intellectual property and cybersecurity law, where she has advised leading corporate institutions on legal measures to be implemented to secure their cyber environment.

Gikera & Vadgama Advocates (GVA) is among the leading legal firms in Africa and continues to expand through its established strategic partners. GVA is truly a comprehensive law firm, uniquely positioned to assist its clients achieve their ambition in an increasingly competitive economy. Its head office is in Nairobi with branches in Mombasa and Nanyuki. Through its strategic partners, GVA has a presence in South Africa, Congo, Nigeria, Ghana, Zimbabwe, Rwanda, Tanzania, Uganda, Ethiopia, Mauritius, the Republic of Chad, Sri Lanka and the UAE.

Our Intellectual Property Law practice is at the heart of GVA and was recently ranked Top 5 by the *Patent Lawyer* magazine. We have advised leading banking and corporate institutions on legal measures that should be implemented to secure their cyber environment, naturally placing us at an advantage with respect to cybersecurity.

Our specialist industry knowledge coupled with our expertise ensures that we can provide cost-effective advice that is innovative and value-adding.

Korea

Seung Soo Choi

JIPYONG LLC

Seungmin Jasmine Jung

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Under the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (the "Network Act"), it is prohibited for anyone to infiltrate another's information communication network ("ICN") without authorised access or beyond the scope of authorised access. Any violation shall be subject to imprisonment of not more than five years or a penalty of not more than KRW 50 million. In a recent court decision, the defendant who infiltrated another's ICN in order to distribute malware was subject to imprisonment of 18 months.

Under the Electronic Financial Transactions Act (the "EFTA"), any unauthorised access of electronic financial systems shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

Denial-of-service attacks

Under the Network Act, it is prohibited to cause disruption of an ICN by intentionally disturbing network operations with large volumes of signal/data or superfluous requests. Any violation shall be subject to imprisonment of not more than five years or a penalty of not more than KRW 50 million.

Also, under the EFTA, any attacks on electronic financial systems using programs such as a computer virus, logic bomb or email bomb with the intention of destroying data on, or disrupting the operation of, electronic financial systems shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

Phishing

For the regulation of phishing crimes, the Special Act On The Prevention Of Loss Caused By Telecommunications-Based Financial Fraud And Refund For Loss (the "Special Act on Financial Fraud") has been enacted. Under the Special Act on Financial Fraud, anyone found guilty of phishing crimes shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Under the Network Act, it is prohibited for anyone to transmit or distribute malware that can damage, destroy, alter, falsify or disrupt the operation of ICN systems, data or programs, without a justifiable cause. Any violation shall be subject to imprisonment of not more than seven years or a penalty of not more than KRW 70 million.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

The use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools) is prohibited under the Network Act. Any violation shall be subject to imprisonment of not more than seven years or a penalty of not more than KRW 70 million.

Identity theft or identity fraud (e.g. in connection with access devices)

Under the Personal Information Protection Act ("PIPA"), anyone who commits, or aids and abets, the illegitimate acquisition of personal information, being processed by another party for subsequent provision to a third party for commercial gain or for illegitimate purposes, shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

Also, under the Network Act, it is prohibited for anyone to collect another person's information, or induce the provision of another person's information, through the ICN by deceptive means. Any violation shall be subject to imprisonment of not more than three years or a penalty of not more than KRW 30 million.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Any theft of the company's critical information by a company's employee or former employee shall be punished under the Criminal Act as a breach of fiduciary duty or under the Act on Prevention of Unfair Competition and Protection of Trade Secrets as divulging of trade secrets. Any such theft shall be subject to imprisonment of not more than 10 years or a penalty of not less than KRW 30 million under the Criminal Act and imprisonment of not more than five years or a penalty of not more than KRW 50 million under the Act on Prevention of Unfair Competition and Protection of Trade Secrets. Any infringement of the employer's copyright shall be subject to imprisonment of not more than five years or a penalty of not more than KRW 50 million.

There have been several cases where a former employer was criminally prosecuted for taking, without permission, material assets or intellectual property rights of the employer upon termination of employment.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Under the Network Act, it is prohibited for anyone to damage another person's information processed, stored or transmitted through the

ICN or to infringe, exploit or disclose another person's confidential information.

Under the EFTA, anyone who falsifies or alters access means shall be subject to imprisonment of not more than seven years or a penalty of not more than KRW 50 million.

Failure by an organisation to implement cybersecurity measures

Under PIPA and its Enforcement Decree, personal information processors have the obligation to implement technical, managerial and physical measures in order to procure security, such as establishing internal control plans and storing access records to ensure personal information is not lost, stolen, leaked, falsified, altered or damaged. In the event personal information is lost, stolen, leaked, falsified, altered or damaged due to a person's failure to implement such measures, such person shall be subject to imprisonment of not more than two years or a penalty of not more than KRW 20 million.

1.2 Do any of the above-mentioned offences have extraterritorial application?

As of yet, there are no regulations regarding extraterritorial application of the above offences.

There is, however, a prohibition of the overseas transfer of personal information. Under PIPA, personal information processers are prohibited from entering into contracts regarding the overseas transfer of personal information with terms in violation of PIPA. "Overseas transfer" is a broad concept dealing with the "actual" transfer of personal information and does not only include the provision of personal information to third parties, but also includes (i) the delegation of personal information processing to a third party located outside of Korea, and (ii) the overseas transfer of personal information due to business transfers or mergers.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

In relation to criminal prosecution of personal information leakage accidents, the responsible party may be discharged from liability if requisite measures for procuring security have been implemented or if due care has been exercised and supervision has been properly conducted.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Under the Act On The Protection Of Information And Communications Infrastructure (the "PICIA"), it is prohibited to disrupt or paralyse critical ICN infrastructure facilities such as electronic control or managerial systems related to national security, government administration, military defence, policing, finance, telecommunications, transportation and energy. Any violation shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The following are Applicable Laws in Korea: Personal Information Protection Act ("PIPA"); Act On The Protection Of Information And Communications Infrastructure (the "PICIA"); Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (the "Network Act"); Electronic Financial Transactions Act (the "EFTA"); Credit Information Use and Protection Act (the "Credit Information Act"); Act on the Protection, Use, etc. of Location Information; Act On Prevention Of Divulgence And Protection Of Industrial Technology; and Special Act On The Prevention Of Loss Caused By Telecommunications-Based Financial Fraud And Refund For Loss (the "Special Act on Financial Fraud").

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Under the PICIA, managerial organisations have the obligation to establish and implement managerial measures, including physical and technical measures (such as prevention, backup, recovery, etc.), to safely protect the critical ICN infrastructure facilities and managerial data.

Under the Network Act, any ICN service provider must take protective measures to procure the security of ICN used in the provision of ICN services and the reliability of information.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Organisations that operate and manage collective ICN facilities ("Collective ICN Facility Operator") for the ICN service of third parties must take the following protection measures (as prescribed under the Enforcement Decree of the Network Act) for the secure operation of ICN facilities:

(i) technical and managerial measures for access control and monitoring of unauthorised access to ICN facilities;

(ii) physical and technical measures for the protection of ICN facilities from natural disasters and threats, such as terrorist attacks, and for procuring the continuous and secure operation of ICN facilities;

(iii) hiring and assignment of personnel for the secure management of ICN facilities;

(iv) establishment and implementation of internal control measures (including emergency plans) for the secure management of ICN facilities; and

(v) establishment and implementation of technical and managerial measures to prevent the dissemination of infiltration Incidents.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

No conflict of laws issues have arisen yet.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Under the Network Act, the ICN provider or a Collective ICN Facility Operator must report any "infiltration Incidents" (defined as Incidents due to attacks on the ICN or the related information system through hacking, a computer virus, logic bomb, email bomb, denial of service, high-powered electromagnetic wave, etc.) to the Ministry of Science and ICT or Korea Internet and Security Agency ("KISA") immediately upon the occurrence of such infiltration Incident.

Under PIPA, in the event of any leakage of personal information which concerns 10,000 or more persons, the personal information processor must report such leakage and subsequent measures, without delay, to the Ministry of Interior and Safety or KISA.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Although not obligated, it would be possible for organisations to voluntarily share information related to Incidents with regulatory authorities.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Under PIPA, once a personal information processer becomes aware of any leakage of personal information, it must notify the owner of the leaked personal information, without delay, of the following:

(i) the type of personal information that has been leaked;

(ii) the timing and circumstances of the leakage;

(iii) the actions that the owner of the personal information can take to minimise any damages resulting from the leakage;

(iv) the protective response measures taken by the personal information processor and relief procedures; and

(v) the name and contact of the department to which the owner of the leaked personal information (who has incurred damages) can file a report.

Under the Credit Information Act, in the event of any credit information leakage, the above items must be notified to the owner of such credit information.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, the responses do not differ.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Ministry of the Interior and Safety, the Ministry of Science and ICT, the Financial Services Commission, and KISA.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

If the requirements under Applicable Laws are not complied with, the relevant authorities may impose a monetary fine. For example, a business that fails to provide notice of a credit information leakage Incident shall be subject to a monetary fine of not more than KRW 50 million.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Order the submission of relevant materials and inspections, a corrective order, criminal charges, etc.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

There are certain variances under Applicable Laws. Under PIPA, the requirements for information security measures to be adopted by personal information processors differ based on the size of the corporation. Moreover, the requirements for protective measures under the Network Act for ICN service providers and under the Credit Information Act for financial institutions are generally stricter than the common requirements.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

With regards to the financial services sector, the Credit Information Act and the EFTA prescribe specific legal requirements for financial institutions.

With regards to the telecommunications sector, the following companies need to obtain a certification as to whether they satisfy the prescribed technical and physical protective measures for the security and reliability of ICNs:

(i) companies such as telecommunication providers or companies who provide information through the telecommunication provider's ICN, whose annual revenue or income is not less than KRW 150 billion; or

(ii) companies such as telecommunication providers or companies who provide information through the telecommunication provider's ICN, whose revenue for the preceding fiscal year is not less than KRW 10 billion or whose average volume of daily users for a three-month period is not less than 1 million.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Unless there are special circumstances, the Representative Director or the CPO (or CISO) shall be liable for any breach of the protective measures prescribed under PIPA, the Network Act and the Credit Information Act.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Under the Network Act, ICN service providers with no fewer than 1,000 employees must appoint a CISO at the senior management level to ensure the security of the ICN system and the secure management of data. The CISO is responsible for the following:

(i) the establishment and management/operation of information protection procedures;

(ii) the analysis/evaluation and improvement of any vulnerabilities in information protection;

(iii) the prevention of and response to infiltration Incidents;

(iv) the establishment of preventive measures for information protection and the architecture/implementation of security measures;

(v) the assessment of preventive security measures for information protection;

(vi) the encryption of critical information and assessments of the adequacy of secure servers; and

(vii) the performance of other information protection measures prescribed under Applicable Laws.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Under the Network Act, in order to analyse the cause of the infiltration Incident, the Minister of Science and ICT can order the ICN provider and the Collective ICN Facility Operator to:

(i) retain relevant material such as records of access to the ICN;

(ii) submit the relevant material; and

(iii) allow physical access to the business site to investigate the cause of the infiltration Incident.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

The government may enforce measures against ICN service providers or its users to prevent an offshore leakage of material information related to national industry, the economy and science/technology through ICN overseas disclosure.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In the event the owner of personal information incurs damages due to the violation of PIPA by the personal information processor, such owner of personal information can claim damages against the personal information processor. The personal information processor will be liable unless it can prove that there was no wilful misconduct or negligence attributable to it. If the owner of personal information incurs damages arising from the loss, theft, leak, falsification, alteration or damage of personal information caused by the wilful misconduct or gross negligence of the personal information processor, the court may award up to treble damages. Also, the owner of the personal information may seek statutory damages up to KRW 3 million in the event that loss, theft, leak, falsification, alteration or damage of personal information is caused by the wilful misconduct or gross negligence of the personal information processor. In such case, the personal information provider will be liable unless it can prove that there was no wilful misconduct or negligence attributable to it.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

In 2014, there was a large-scale leakage of personal information from three major credit card companies. The victims of the leakage, as the plaintiffs, brought a case against the credit card companies and the court awarded damages in the amount of KRW 10,000 to each of the plaintiffs for each Incident of leakage.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

In cases regarding tort liability, the plaintiff has the burden of proof with respect to the tort of the defendant. However, in cases claiming damages for leakage of personal information or credit information,

the defendant has the burden of proof to show that the Incident is not attributable to the defendant. In other words, the burden of proof is reversed.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Under the Credit Information Act, certain financial institutions have the obligation to take measures, such as taking out insurance, joining a cooperative, or setting aside a reserve to procure funds for damages that may arise due to credit information leakage.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

The Financial Supervisory Service has set a minimum insurance coverage limit for the liability of financial institutions against credit information leakage. For example, in the case of banks, such limit is KRW 2 billion.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

Under the Act On The Promotion Of Workers' Participation And Cooperation, any installation of monitoring facilities require consultation with the Employee and Employer Council. The Employee and Employer Council is a body established within a company for the purpose of promoting the workers' welfare and the advancement of the company through the participation and cooperation of both the employee and employer.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no specific requirements under Applicable Laws.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The following authorities have investigatory powers of law enforcement: National Intelligence Service; National Police Agency Cyber Bureau; Forensic Science Investigation Department of the Supreme Prosecutors' Office; Financial Supervisory Service; and KISA.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no specific requirements under Applicable Laws.

Seung Soo Choi
JIPYONG LLC
10F, KT&G Seodaemun Tower
60 Chungjeong-ro, Seodaemun-gu
Seoul 03740
Korea

Tel: +82 2 6200 1759
Fax: +82 2 6200 0820
Email: sschoi@jipyong.com
URL: www.jipyong.com/en

Mr. Seung Soo Choi is a Partner and Head of the IT/IP Practice Group at JIPYONG LLC. Mr. Choi has advised and represented IT companies and start-ups on copyright, patent and IP cases and has also handled a variety of litigations over the last 20 years, covering civil, criminal and commercial cases. With his significant amount of working-level experience, he is recognised as the leading expert in the areas of intellectual property and IT, patents, confidential business information, related to copyrights and trademarks.

Mr. Choi is well-acquainted with laws relating to cultural art and entertainment/media businesses and personal information protection. Mr. Choi actively participates in various academic societies and lectures courses on international entertainment law, motion pictures law, art law, data privacy law, communication law, and media law at Chung-Ang University Law School. Mr. Choi is also a well-recognised mediator in the area of entertainment at the Korean Commercial Arbitration Board.

Mr. Choi is a member of the Korean Bar and received an LL.B. from Seoul National University and the University of Pennsylvania.

Seungmin Jasmine Jung
JIPYONG LLC
10F, KT&G Seodaemun Tower
60 Chungjeong-ro, Seodaemun-gu
Seoul 03740
Korea

Tel: +82 2 6200 1712
Fax: +82 2 6200 0820
Email: smjung@jipyong.com
URL: www.jipyong.com/en

Ms. Seungmin Jasmine Jung is a Senior Foreign Attorney in the Finance Practice Group and IP·IT Practice Group of JIPYONG LLC.

Ms. Jung represents clients in the finance, fintech, energy, real estate and technology sector and has extensive experience in acquisition finance, project finance, structured finance, derivatives, data privacy, private equity fund investments and M&A transactions. She is also considered one of the foremost experts on cloud computing, cryptocurrency, blockchain and cybersecurity.

Prior to joining JIPYONG, Ms. Jung was the Head of Legal at Amazon Web Services Korea, where she specialised in cloud computing and data privacy. Ms. Jung started her legal career as an associate at the NY office of Hughes, Hubbard & Reed and subsequently worked at Shin & Kim and Franklin Templeton Investments in Seoul, Korea.

Currently, Ms. Jung regularly advises clients on cryptocurrency, blockchain and cloud computing while frequently lecturing at conferences, and contributing articles on legal issues surrounding the 4th Industrial Revolution. Ms. Jung also teaches technology law at Yonsei University, her *alma mater*. She is highly regarded by her clients for her transactional expertise and strong negotiation skills.

Ms. Jung is a member of the New York Bar. Ms. Jung has a J.D. from Columbia Law School and a B.A. in political science and international relations from Yonsei University.

JIPYONG JIPYONG LLC

JIPYONG LLC is one of Korea's leading full-service law firms. We pride ourselves on our global reach and outlook, the depth and breadth of our practice groups and the extensive experience of our lawyers. With our network of 12 international offices and desks in China, Russia, Vietnam, Indonesia, Myanmar, Cambodia, Laos and Iran, etc., we provide a one-stop destination for legal and consulting services to our clients. JIPYONG LLC has a strong base of domestic and international clients who rely on us for not only our local market knowledge and expertise but for our innovative, business-minded solutions. In addition to our pursuit of professional excellence and proactively serving the needs of clients, JIPYONG LLC shares an unwavering commitment to high ethical standards, *pro bono* work and community service.

Kosovo

Genc Boga

Boga & Associates

Delvina Nallbani

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Law No. 03/L-166 "On prevention and fight of the cyber crime" ("Cyber Crime Law") provides for criminal offences related to the misuse of computer systems and computer data, although it does not provide a literal denomination of the criminal offences listed below.

Hacking (i.e. unauthorised access)

Subject to the Cyber Crime Law, unauthorised access to computer systems constitutes a criminal offence, punishable by imprisonment for up to three years. Unauthorised actions are classified actions performed by a person: (i) who is not authorised by law or contract; (ii) who exceeds the limits of his/her authorisation; and/or (iii) has no permit and is not competent and qualified to use, administer or control a computer system or conduct scientific research on a computer system.

If such an offence is committed for the purpose of obtaining computer data or violates computer security measures, the penalties provided by law are higher and such offences are punishable by imprisonment for up to four years and five years, respectively.

In addition, the Criminal Code (Law No. 04/L-082) provides for the criminal offence of unauthorised access of computer systems. In this regard, whoever, without authorisation and in order to gain an unlawful material benefit for himself or another person or to cause damage to another person, alters, publishes, suppresses or destroys computer data or programs, or in any other way enters another's computer system, is punished by a fine and up to three years of imprisonment. If the offence results in a material gain exceeding 10,000 Euros or material damage exceeding 10,000 Euros, the perpetrator shall be punished by a fine and by imprisonment of up to five years.

Denial-of-service attacks

The serious hindrance of the functioning of computer systems, performed by entering information, transferring, changing, removing or destroying computer data or unauthorised limiting of access to such data, is stipulated as a criminal offence pursuant to the Cyber Crime Law, and the perpetrator is liable to imprisonment for up to three years. Such offence shall be punished by imprisonment for up to five years if committed by a member of a criminal organisation.

Phishing

We have not identified a criminal offence provided by the Cyber Crime Law or other applicable laws that would represent phishing. However, each criminal activity that aims to misuse computer systems or computer data should be considered individually to establish whether it constitutes a criminal offence provided for by the Cyber Crime Law or any other applicable law.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

We have not identified a criminal offence provided by the Cyber Crime Law or other applicable laws that would constitute infection of IT systems with malware. However, each criminal activity that aims to misuse computer systems or computer data should be considered individually to establish whether it constitutes some other criminal offence provided for by the Cyber Crime Law or any other applicable law.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Pursuant to the Cyber Crime Law, the illegal production, sale, import, distribution or making available, in any form, of any equipment or computer program designed and adapted for the purpose of committing any criminal offence is punishable by imprisonment from one to four years.

Further, the illegal production, sale, import, distribution or making available, in any form, of passwords, access codes or other computer information that would allow full or partial access to a computer system for the purpose of committing any criminal offence shall be punishable by imprisonment from one to five years.

In addition, the illegal possession of equipment, computer programs, passwords, access codes or computer information for the purpose of committing any criminal offence is punishable by imprisonment from one to six years.

An attempt to commit this criminal offence is also punishable by imprisonment, ranging from three months to one year.

Identity theft or identity fraud (e.g. in connection with access devices)

We have not identified any criminal offence provided for by the Cyber Crime Law or other applicable laws that would constitute identity theft or identity fraud. However, as mentioned above, such criminal activities should be assessed individually.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Pursuant to the Criminal Code (Law No. 04/L-082), an act of avoiding any of the effective technological measures to safeguard technology or the removal or alteration of electronic rights for data

management, as provided for by the Law "On copyright and related rights", shall be punishable by imprisonment for up to three years.

Subject to the Law "On copyright and related rights" (Law No. 04/L-065), violation of the rights protected by this law would be considered if a person processes, imports for distribution, sells, lends, advertises for sale or lease or keeps for commercial technological purposes a computer program, or carries out services without authorisation, and if such actions: (i) are advertised or traded especially for the purpose of avoiding effective technological measures; (ii) have evident commercial purpose or have been used solely for avoiding effective technological measures; and (iii) are designed, produced, adapted or processed primarily with the purpose of avoiding effective technological measures. An effective technological measure is considered to be any technology, computer program or other means intended to prevent or remove a violation of a protected right. Pursuant to the Criminal Code (Law No. 04/L-082), an act of avoiding any of the effective technological measures to safeguard technology or the removal or alteration of electronic rights for data management shall be punishable by imprisonment for up to three years.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

In addition to the criminal offences listed above, the Cyber Crime Law also provides for the following criminal offences related to computer systems and computer data: the unauthorised entry of data; change or deletion of computer data; and the unauthorised limitation of access to such a data resulting in inauthentic data.

Also, causing a loss in assets to another person by entering information, changing or deleting computer data by means of access limitation to such a data, or any other interference into the functioning of a computer system with the purpose of ensuring economic benefits for himself or for someone else, shall be punishable with up to 10 years of imprisonment.

Failure by an organisation to implement cybersecurity measures

We have not identified such a criminal offence provided for by the applicable legislation.

1.2 Do any of the above-mentioned offences have extraterritorial application?

In addition to the criminal offences committed within the Kosovo territory, the abovementioned laws that stipulate criminal offences will also apply to persons who have committed criminal offences outside the territory of Kosovo, if provided for by an international agreement by which Kosovo is bound.

Criminal legislation of the Republic of Kosovo shall also apply to any Kosovo citizen or a foreigner who commits a criminal offence outside the territory of the Republic of Kosovo if the criminal offence is also punishable in the country where the offence was committed. In case of foreigners, these provisions shall apply if the foreigner is found in the territory of Kosovo or has been transferred to Kosovo.

However, the criminal proceedings against a Kosovo citizen or a foreigner for criminal offences committed outside Kosovo territory will not be undertaken if the perpetrator has fully served the punishment imposed in another jurisdiction, has been acquitted by a final judgment and/or released from punishment or punishment has become statute-barred and in cases where criminal proceedings may only be initiated upon the request of the injured party and such a request has not been filed.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Subject to article 8 of the Cyber Crime Law, for a category of computer systems to which access is restricted or completely forbidden, the owners and administrators of such a computer system are obliged to clearly and automatically warn the user of this computer system, and to provide him/her with information, as well as conditions of use, or forbiddance to use this computer system and legal consequences for unauthorised access to this computer system. Failure to comply with such an obligation is considered a misdemeanour and the perpetrator is punished with a fine ranging from 500 to 5,000 Euros.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

The Criminal Code provides that issuing blank or false cheques and the misuse of bank or credit cards constitutes a criminal offence. Such an offence is defined as an act committed for the purpose of gaining unlawful material benefit for the perpetrator or for another person, by issuing or placing into circulation cheques for which the perpetrator knows are not covered by material means. The placing of false cheques or counterfeit credit cards is punished by a fine and imprisonment for up to three years. In relation to prosecution of this criminal offence in a cybersecurity context, there is a case pending before Kosovo courts where the defendant has been prosecuted for violation of the Cyber Crime Law, specifically for the possession or use of passwords, hardware, software or other tools to commit cybercrime.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The Applicable Laws relevant to cybercrime are listed below.

Law No. 03/L-166 "On prevention and fight of the cyber crime"; Law No. 04/L-082 "Criminal Code of The Republic Of Kosovo", as amended by Law No. 04/L-129 and Law No. 04/L-273; Law No. 04/L-094 "On the information society services"; Law No. 04/L-109 "On electronic communications"; Law No. 05/L-030 "On interception of electronic communication"; Law No. 03/L-172 "On the protection of personal data"; Law No. 04/L-149 "On the execution of penal sanctions", as amended by Law No. 05/L-129; Law No. 04/L-065 "On copyright and related rights" as amended by Law No. 05/L -047; Law No. 04/L-093 "On banks, microfinance institutions and non bank financial institutions"; Law No. 04/L-198 "On the trade of strategic goods"; Code No. 03/L-109 "Customs and excise code of Kosovo" as amended by the Law No. 04/L-099; and Law No. 03/L-178 "On classification of information and security clearances".

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Kosovo is not an EU member; however, the Ministry of Internal Affairs has adopted the State Strategy for Cyber Security and the Action Plan for 2016 to 2019, drafted based on European Union practices and policies.

The Kosovo Government has also made the Kosovo Police available as a permanent contact point for international cooperation in the field of cybercrime. In this regard, the Kosovo Police should ensure ongoing international cooperation and assistance in the field of cybercrime, order data retention and confiscation of equipment containing data, as well as cooperate with all competent Kosovo authorities while undertaking execution actions.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The Cyber Crime Law provides that authorities and public institutions with competence in this area, service providers, non-governmental organisations and civil society representatives should carry out activities and programmes for the prevention of cybercrime and develop policies, practices, measures, procedures and minimum standards for the security of computer systems and should also organise information campaigns on cybercrime and risks for computer system users.

The Ministry of Justice, the Ministry of Internal Affairs, the Ministry of Transport and Communications, the Ministry of Public Services, and the Kosovo Intelligence Services shall develop special training programmes for personnel for the purpose of preventing and fighting cybercrime in accordance with specific competencies.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

We have not identified any provisions that could lead to conflicts of laws issues. However, in certain cases, the provisions of Law No. 05/L-030 "On interception of electronic communications", which govern the procedures and conditions for authorised interception of electronic communications, may come into conflict with the measures for surveillance, detection, prevention or mitigation of an Incident by authorised authorities in the cybercrime area.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There is no obligation to report information related to Incidents to a special authority in Kosovo. However, the Cyber Crime Law provides that the Ministry of Justice, in cooperation with the Ministry of Internal Affairs, shall continuously maintain and supplement the database on cybercrime.

In principle, in order to report any criminal offence, a criminal complaint may be filed by any person to the police station in the area where the crime was committed or to the competent state prosecutor in writing, by technical means of communication or orally. For practical reasons, criminal offences are typically reported to the police station.

After receiving information of a suspected criminal offence, the police shall investigate whether there is reasonable suspicion that a criminal offence prosecuted *ex officio* has been committed. The police shall investigate a criminal complaint and shall take all the necessary steps (i.e. to locate the perpetrator, to prevent, detect and preserve traces and other evidence, to collect all the information that may be of use in criminal proceedings, etc.). In order to perform these tasks, the police are authorised, under the provisions of the Criminal Procedure Code (Law No. 04/L-123), to gather information from individuals, to take all the necessary steps to establish the identity of the persons, and to interview witnesses or possible suspects, etc.

Based on such collected information, the police drafts the criminal complaint and submits it to the competent state prosecutor. The public prosecutor is obliged to act according to the criminal complaint, i.e. to initiate proceedings (file an indictment) or to dismiss the criminal complaint.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

The applicable legislation is silent in this regard.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Subject to the Cyber Crime Law, the prosecutor is obliged to notify in writing, by the end of the investigation, the persons who are under investigation.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The applicable legislation does not address this issue.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The State Prosecutor and the Courts are the institutions responsible for the prosecution and punishment of perpetrators of criminal offences and for the confiscation of property acquired through criminal offences.

Also, listed below are institutions relevant to the cybercrime area:

- The Ministry of Internal Affairs is responsible for the drafting and monitoring of policies and legislation in the field of overall security and cybersecurity.
- The Kosovo Police, as a law enforcement agency, has the primary responsibility in combatting all forms of cybercrime within the Cybercrime Sector and for implementing specific supporting structures. The Kosovo Police also serves as a contact point for international cooperation in the field of cybercrime.
- The Kosovo Security Council Secretariat, as an integral part of the Kosovo Security Council, prepares periodic reports for the Government of the Republic of Kosovo and the Kosovo Security Council dealing with security policy issues.
- The Kosovo Intelligence Agency identifies threats that endanger Kosovo's security, such as the threat to territorial integrity, institutional integrity, constitutional order, stability and economic development, as well as threats to global security to the detriment of Kosovo.
- The National Agency for the Protection of Personal Data ensures that controllers respect their obligations regarding the protection of personal data and that data subjects are informed about their rights and obligations in accordance with the Law "On protection of personal data".
- The Ministry of Justice, the Ministry for the Kosovo Security Force, the Ministry of Economic Development, the Ministry of Foreign Affairs, the Ministry of Finance, as well as the Regulatory Authority of Electronic Data and Postal Communications and the Information Society Agency contribute to cybersecurity in their relevant fields.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

There are no penalties provided for by the applicable legislation.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

We are not aware of any enforcement actions taken in this area.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

There is no consolidated practice in the area of cybercrime to make this assessment.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

There are no specific requirements as regards to cybersecurity in different organisations. However, as regards the telecommunication sector, there are specific obligations for the purpose of criminal proceedings for entrepreneurs of public electronic communications services and networks based on the Law "On electronic communications" (Law No. 04/L-109). As regards the financial sector, financial institutions in Kosovo are bound by the provisions of the Law "On the prevention of money laundering and combating financing of terrorism" (Law No. 05/L-096), which provides measures and procedures for detecting and preventing criminal offences of money laundering and combatting terrorist financing.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

We have not identified such circumstances based on the applicable legislation.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There is no such responsibility provided under the Applicable Laws for companies.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No, they are not.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, they are not.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Civil actions that may be brought would be those claiming compensation of damages in virtue of the Law "On obligations relationship" (Law No. 04/L-077). In that case, the culpability of a person that has caused damages in relation to any Incident should be proven.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

From the review of some of the published decisions of the Basic Courts and the Supreme Court adopted during 2017 and 2018, we have not identified any decision adopted in this respect. Based on media reports, there have been several cases of prosecution for possession or use of passwords, software or other tools to commit cybercrime, prosecuted in connection with the criminal offence of abuse of banks and credit cards.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

There are no such liabilities provided under Kosovo law.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Such a type of insurance does not exist in practice.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no such regulatory limitations provided by the Applicable Laws.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There are no such requirements provided by the applicable legislation.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

We have not found any provisions in the Law "On witness protection" (Law No. 04/L-015) that may limit the reporting of Incidents. The law provides for special and urgent measures and procedures for witness protection if there is a serious threat to a person and the person's close relatives and if that person agrees to cooperate closely with the courts or investigatory authorities.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Pursuant to the Criminal Procedure Code (Law No. 04/L-123), the state prosecutor may undertake investigative actions or authorise the police to undertake investigative actions regarding the collection of evidence. In the latter case, the police shall investigate criminal offences and shall take all the steps necessary to locate the perpetrator, to prevent the perpetrator or his/her accomplice from hiding or fleeing, to detect and preserve traces and other evidence of the criminal offence and objects which might serve as evidence, and to collect all the information that may be of use in the criminal proceedings.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no such requirements.

Genc Boga
Boga & Associates
40/3 Ibrahim Rugova Str.
1019 Tirana
Albania

Tel: +355 4 2251 050
Email: gboga@bogalaw.com
URL: www.bogalaw.com

Genc Boga is the founder and Managing Partner of Boga & Associates, which operates in the jurisdictions of both Albania and Kosovo. Mr. Boga's fields of expertise include business and company law, concession law, energy law, corporate law, banking and finance, taxation, litigation, competition law, real estate, environment protection law, etc.

Mr. Boga has solid expertise as advisor to banks, financial institutions and international investors operating in major projects in energy, infrastructure and real estate. Thanks to his experience, Boga & Associates is retained as a legal advisor on a regular basis by the most important financial institutions and foreign investors.

He regularly advises EBRD, IFC and World Bank in various investment projects in Albania and Kosovo.

Mr. Boga is continuously ranked as a leading lawyer in Albania by major legal directories: *Chambers Global*, *Chambers Europe*, *The Legal 500* and *IFLR 1000*.

He is fluent in English, French and Italian.

Delvina Nallbani
Boga & Associates
27/5 Nene Tereza Str.
10000 Pristina
Kosovo

Tel: +383 38 223 152
Fax: +383 38 223 153
Email: dnallbani@bogalaw.com
URL: www.bogalaw.com

Delvina Nallbani is a Senior Associate at Boga & Associates, which she joined in 2012.

Her practice is mainly focused on providing legal advice to clients on a wide range of corporate, mergers and acquisitions, business and banking matters. She also provides assistance in advising investors on a number of transactions including project finance, mergers and acquisitions, and privatisations.

Delvina graduated in law from the University of Zagreb, and is member of the Kosovo Bar Association.

She is fluent in Croatian and English.

BOGA & ASSOCIATES

LEGAL • TAX • ACCOUNTING

Boga & Associates, established in 1994, has emerged as one of the premier law firms in Albania, earning a reputation for providing the highest quality of legal, tax and accounting services to its clients. The firm also operates in Kosovo (Pristina) offering a full range of services. Until May 2007, the firm was a member firm of KPMG International and the Senior Partner/Managing Partner, Mr. Genc Boga, was also the Senior Partner/Managing Partner of KPMG Albania.

The firm's particularity is linked to the multidisciplinary services it provides to its clients, through an uncompromising commitment to excellence. Apart from the widely consolidated legal practice, the firm also offers the highest standards of expertise in tax and accounting services, with keen sensitivity to the rapid changes in the Albanian and Kosovo business environment.

The firm delivers services to leading clients in major industries, banks and financial institutions, as well as to companies engaged in insurance, construction, energy and utilities, entertainment and media, mining, oil and gas, professional services, real estate, technology, telecommunications, tourism, transport, infrastructure and consumer goods.

The firm is continuously ranked as a "top tier firm" by major directories, such as: *Chambers Europe*; *The Legal 500*; and *IFLR 1000*.

Malaysia

Deepak Pillai

Christopher & Lee Ong

Yong Shih Han

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes. Under section 3 of the Computer Crimes Act 1997 ("**CCA**"), it is an offence if a person knowingly and intentionally accesses a computer without authorisation and causes a computer to perform any function with the intent to secure access to any program or data held in any computer.

A person found guilty of an offence under section 3 is liable to a fine not exceeding RM50,000 or imprisonment not exceeding five years or both.

In *PP v Vishnu Devarajan* [2016] 1 LNS 1066, the accused was charged under section 3 of the CCA for accessing without authorisation the servers of a broadcast centre and the server database of a Malaysian radio network company. However, all charges were dropped due to technical and procedural errors in the prosecution of the case.

Section 4 of the CCA creates a further offence against persons who commit a hacking offence under section 3 with the intent to: (i) commit an offence involving fraud or dishonesty which causes injury under the Malaysian Penal Code (the main penal statute in Malaysia) (the "**Penal Code**"); or (ii) facilitate the commission of such an offence whether by himself or any other person. A person found guilty under section 4 is liable to a fine not exceeding RM150,000, or imprisonment not exceeding 10 years, or both.

In *Basheer Ahmad Maula Sahul Hameed v PP* [2016] 6 CLJ 422, the two accused persons, who were husband and wife, where the wife worked in a bank, were convicted under section 4(1) of the CCA for using a debit card belonging to an airplane accident victim to withdraw cash from an ATM machine and for transferring money from several other victims' online banking accounts without authorisation.

Denial-of-service attacks

There is no specific provision which provides for denial-of-service attacks. However, under section 233(1)(b) of the Communications and Multimedia Act 1998 ("**CMA**"), a person who continuously, repeatedly or otherwise initiates a communication using any applications services with the intent to annoy, abuse, threaten or harass any person at any number or electronic address commits an offence, regardless of whether the communication ensued and whether or not the person initiating such communication disclosed their identity.

A person found guilty of an offence under section 233(1)(b) is liable to a fine not exceeding RM50,000, or imprisonment not exceeding one year, or both, and shall also be liable to a further fine of RM1,000 for every day that the offence is continued after conviction.

To date, there have been no reported cases under section 233(1)(b) of the CMA.

Phishing

There are no specific offences with regard to phishing. However, other statutory provisions may be applicable in tackling phishing offences.

Under section 416 of the Malaysian Penal Code, any person is said to "cheat by personation", if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is. The offence of cheating by personation is punishable with imprisonment for a term which may extend to seven years and/or a fine.

To date, there are no reported cases specifically in relation to phishing.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Infection of IT systems with malware is an offence punishable under the CCA. Under section 5 of the CCA, it is an offence for a person to do any act which he knows will cause unauthorised modification of the contents of any computer.

A person found guilty of an offence under section 5 is liable to a fine not exceeding RM100,000 or imprisonment not exceeding 10 years, or both if the act was done with the intention of causing injury.

In *PP v Roslan and Anor* [2016] 1 LNS 651, the accused who worked as a Systems Analyst in the IT Department of the Malaysian Hajj Pilgrims Fund Board, was convicted under section 5(1) of the CCA for modifying pilgrims' records in the organisation's database without authorisation.

In *PP v Vishnu Devarajan* [2016] 1 LNS 1066, the accused was charged under section 5 of the CCA for, amongst others, carrying out the following without authorisation: downloading and launching software; running and stopping certain processes on servers; and running certain programs on the database server of a broadcast centre. However, all charges were dropped due to technical and procedural errors in the prosecution of the case.

In *Kangaie Agilan Jammany v PP* [2017] 1 LNS 1640, the accused, an employee of AirAsia, a low-cost airline carrier company, was charged under section 5 of the CCA where he used the Air Asia reservation system without authorisation to modify passenger flight

schedules, in order to help family members and friends obtain airline tickets at lower rates.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Under section 236 of the CMA, it is an offence for a person to possess or use any counterfeit access devices, unauthorised access devices (e.g. lost, stolen, expired, or obtained with the intention to defraud), any device-making equipment intended to make counterfeit access devices, or any other equipment or device modified or altered or intended to alter or modify such other equipment or device in order to obtain unauthorised access to any network services, etc.

Possession or use of the above is an offence and the offender would be liable to a fine not exceeding RM500,000 or to imprisonment not exceeding five years, or both.

Under section 240 of the CMA, it is an offence to distribute or advertise any communications equipment or device for interception of communication. An offence under this section would render the offender liable to a fine not exceeding RM100,000 or to imprisonment not exceeding two years, or both.

To date, there have been no reported cases under either section 236 or section 240 of the CMA.

Identity theft or identity fraud (e.g. in connection with access devices)

The Penal Code contains provisions on cheating by personation. Although not cyber-specific, section 416 of the Penal Code (as discussed above) may apply to identity theft. Under section 416 of the Penal Code, it is an offence to "cheat by personation", i.e. where a person cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such person really is.

To date, while there has been news of individuals committing identity theft or fraud, such cases have, however, usually been tried on the basis of contravening national registration regulations (in relation to impersonating or theft of identification cards). There have been no reported cases for actions on identity theft or identity fraud specifically in the context of cybersecurity or cybercrimes.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Under Malaysian law, the right to bring an action for breach of confidence stems from common law, or pursuant to the contracts of employment, which generally contain confidentiality clauses and as such would not constitute a criminal offence.

Copyright owners have the right to bring an action for copyright infringement either as a civil or criminal offence. Section 41 of the Copyright Act 1987 sets out a range of offences for copyright infringement, which include making for sale or hire, distributing, and exhibiting in public any infringing copy during the subsistence of copyright in a work or performers' right.

In *Chuah Gim Seng & More Again v. SO* [2009] 10 CLJ 65, the appellants were found guilty and convicted for the sale of pirated copy films. The penalty imposed was RM2,000 for the sale of each copy and in default a four-month jail term for failure to pay each charge.

In *PP v. Haw Swee Po* [2011] 5 LNS 23, the accused was tried for possession and use (other than for private and domestic use) of 3,300 copies of seven films in DVD format. The court sentenced the accused to 14 months' imprisonment.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Activities which adversely affect or threaten security, confidentiality, integrity or availability of IT systems, infrastructures, etc. are prohibited or regulated under the CMA. For example, it is an offence to: use any apparatus or device with the intent to obtain information regarding the contents, sender or addressee of any communication without an approval by a registered certifying agency (section 231 of the CMA); possess or create a system designed to fraudulently use or obtain any network facilities, network service, applications service or content applications service (section 232(2) of the CMA); intercept, attempt to intercept, or procure any other person to intercept or attempt to intercept, any communications (section 234 of the CMA); and extend, tamper with, adjust, alter, remove, destroy or damage any network facilities or any part thereof (section 235 of the CMA).

A person who is found liable for any of the above offences under CMA may, upon conviction, be held liable to a maximum fine ranging from RM50,000 to RM300,000 or imprisonment not exceeding two to three years, or both.

In relation to personal data, organisations are required to ensure the security of individuals' personal data (section 9 of the Personal Data Protection Act 2010, the "**PDPA**"), and in this regard are required to comply with the minimum security standards prescribed by the Personal Data Protection Standards 2015 (the "**PDP Standards**"). Non-compliance with section 9 of the PDPA may hold the offender liable to a fine not exceeding RM100,000 or imprisonment not exceeding two years, or both, whereas non-compliance with any of the security standards under the PDP Standards may result in the offender being held liable to a fine not exceeding RM250,000 or imprisonment not exceeding two years, or both.

To date, there have been no reported cases prosecuted under any of the abovementioned provisions of the CMA or PDPA.

Failure by an organisation to implement cybersecurity measures

There is currently no legislation which imposes a blanket requirement in respect of implementing cybersecurity measures. The closest is the PDPA, which only applies to organisations involved in commercial transactions and expressly excludes the Government of Malaysia.

Organisations that are involved in processing personal data are required to implement minimum security standards as prescribed by the PDP Standards, or such other standards as prescribed by the Personal Data Protection Commissioner (the "**PDP Commissioner**") from time to time.

Certain sectors are additionally subject to the guidelines requiring the implementation of certain cybersecurity measures, for example:

(a) in the capital market industry, capital market entities are subject to cybersecurity requirements as set out in the *Guidelines on Management of Cyber Risk* issued by the Securities Commission of Malaysia ("**SC**"); and

(b) in the banking and financial sector, banks and financial institutions are subject to the requirements as set out in the *Guidelines on Management of IT Environment (GPIS 1)* issued by the Central Bank of Malaysia or Bank Negara Malaysia ("**BNM**").

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes. The CCA, CMA, and to a certain extent, the Penal Code (in relation to terrorism and offences against the state) have extraterritorial application.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

For organisations that are subject to cybersecurity obligations or requirements (e.g. PDPA, sector-specific cybersecurity requirements),

there are no specific actions specified in the statutes or guidelines which might mitigate the penalty which would otherwise be incurred by reason of any breach or non-compliance by the organisation. However, it is reasonable to infer that cooperation with the relevant regulators or enforcement authorities, or active steps taken to mitigate the loss or damage caused by any of the offences, may serve to mitigate the severity of the penalty to be imposed by the regulators or enforcement authorities.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

It is generally an offence (even though not specific to cybersecurity) to commit or facilitate terrorism activities, e.g., where there is financing of terrorism, or participation or indication of support to terrorist groups or activities (section 130J of the Penal Code).

In the context of cyberterrorism, sub-section (2)(k) of section 130J specifically provides that "support" to a terrorist group extends to the act of "using social media or any other means to:

(i) advocate for or to promote a terrorist group, support for a terrorist group or the commission of a terrorist act; or

(ii) further or facilitate the activities of a terrorist group".

While Malaysian enforcement authorities have regularly taken steps to block or remove known terrorist websites, there have been no reported cases in respect of cyberterrorism under the abovementioned section 130J(2)(k) of the Penal Code.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

As at the time of writing, there is no single piece of legislation in Malaysia in respect of cybersecurity. In June 2017, the then Malaysian Home Minister, Ahmad Zahid Hamidi, announced that a new cybersecurity bill will be drafted and tabled in Parliament, in order to combat cybercrimes, including recruitment and financial sourcing by terrorist groups, money laundering and online gambling. However, the cybersecurity bill has not been tabled in Parliament to date.

Notwithstanding the above, the current laws which relate to cybersecurity in Malaysia include:

Communications and Multimedia Act 1998 (CMA)

The CMA provides for and regulates the converging areas of communications and multimedia. In particular, the CMA regulates various activities carried out by licensees (i.e. network facilities providers, network service providers, applications service providers and content applications service providers) as well as those utilising the services provided by the licensees. One of the objects of the CMA is to ensure information security and network reliability and integrity in Malaysia. The CMA: requires licensees to use their best endeavours to prevent network facilities or network services from being used for the commission of any offence under Malaysian laws; prohibits fraudulent or improper use of network facilities or network services; prohibits the use and possession of counterfeit access devices; prohibits use of equipment or device in order to obtain unauthorised access to any network services; and prohibits interception of any communications unless with lawful authority.

Computer Crimes Act 1997 (CCA)

The CCA criminalises: the act of gaining unauthorised access into computers or networks; spreading malicious codes (e.g. viruses, worms and Trojan horses); unauthorised modification of any program or data on a computer; as well as wrongful communication of any means of access to a computer to an unauthorised person. Depending on the type of offence committed, the fine for a convicted offence ranges from RM25,000 to RM150,000 or imprisonment of three to 10 years or both. The case *Basheer Ahmad Maula Sahul Hameed v PP* [2016] 6 CLJ 422 (as discussed in 'Hacking' in question 1.1 above) is an example of an offence under CCA.

Penal Code

In cases where computer-/Internet-related crime activities are involved, but do not specifically fall within the ambit of any of the aforementioned statutes (for example, online fraud, cheating, criminal defamation, intimidation, gambling, pornography, etc.), such offences may be charged under the Penal Code, which is the main statute that deals with a wide range of criminal offences and procedures in Malaysia.

Personal Data Protection Act 2010 (PDPA)

The PDPA regulates the processing of personal data in commercial transactions and applies to anyone who processes and has control over or authorises the processing of any personal data in respect of commercial transactions.

The most relevant PDPA principle in the context of cybersecurity would be the Security Principle, i.e. appropriate technical and organisational security measures must be taken to prevent unauthorised or unlawful processing of personal data and accidental loss, misuse, modification or unauthorised disclosure of personal data.

The PDP Commissioner has also issued subsidiary legislation pursuant to the PDPA, among which are the Personal Data Protection Regulations 2013 (the "**Regulations**") and the Personal Data Protection Standard 2015 (the PDP Standards), which provide specific requirements regarding security standards expected of data users.

Copyright Act 1987 ("Copyright Act")

The Copyright Act generally protects copyrights, including trade secrets, intellectual property in devices or data, etc. Where any technological protection measure is applied to any copyright, it is an offence under the Copyright Act to circumvent such technological protection measures (section 36A of the Copyright Act). No person shall offer such technology or device which allows for circumvention of such technological protection measures, and non-compliance with the provision would be an offence and the person guilty of the offence may be held liable to a fine not exceeding RM 250,000 or to imprisonment for a term not exceeding five years, or to both; and for any subsequent offence, to a fine not exceeding RM 500,000 or to imprisonment for a term not exceeding 10 years, or to both.

Strategic Trade Act 2010 ("Strategic Trade Act")

The Strategic Trade Act 2010 is the legislation that controls the export, trans-shipment, transit and brokering of strategic items and technology, as well as activities that will or may facilitate the design, development, production and delivery of weapons of mass destruction. The Strategic Trade Act, which is consistent with Malaysia's international obligations on national security, prohibits the import or export of strategic items, including items deemed as 'strategic technology' (i.e. controlled items as determined by the Minister of International Trade and Industry in Malaysia, such as encryption technology) (section 9 of the Strategic Trade Act).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The Malaysian Government, under the National Cyber Security Policy ("**NCSP**") has identified 10 critical sectors in Malaysia, known as the Critical National Information Infrastructure ("**CNII**"), which are required to be protected to a level commensurate with the risks faced. These CNII sectors are:

(1) National Defence and Security.
(2) Banking and Finance.
(3) Information and Communications.
(4) Energy.
(5) Transportation.
(6) Water.
(7) Health Services.
(8) Government.
(9) Emergency Services.
(10) Food and Agriculture.

While there are no minimum protective measures in general and across sectors to protect data and information technology systems from Incidents (save for security requirements in relation to personal data under the PDPA), the government of Malaysia has stipulated *ISO/IEC 27001 Information Security Management Systems* ("**ISMS**") as the baseline standard for information security and has proposed for all CNII sectors (as listed above) to be ISMS-certified. Such standards have been incorporated in certain sector-specific guidelines/handbooks. Penalties for failure to undertake such protective measures would be as prescribed by the respective standards/guidelines.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The PDPA regulates processing of personal data in the context of commercial transactions, including for the purpose of ensuring security of such data. Under the Regulations, organisations that process personal data (i.e. data users under the PDPA) are required to develop a security policy to ensure that personal data is protected from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

Further to the above, the PDP Standards prescribe a list of minimum security standards to be complied with by the data users (e.g. prohibition of the use of removable media devices or cloud computing services for transfer or storage of personal data, unless with written authorisation from the top management of the organisation; ensuring the organisation's backup/recovery system and anti-virus software are regularly updated to protect personal data from data intrusion or security breach; contractually binding third-party data processors in respect of data processing activities, etc.).

From the perspective of the CMA in turn, section 263 requires all network facilities or network service providers to use their best endeavours to prevent network facilities or network services, applications services or content applications services from being used in, or in relation to, the commission of any offence under any law of Malaysia.

Apart from the above, several sector-specific standards and guidelines also require organisations to apply security measures. Some examples of these are *Guidelines on Internet Insurance for the Insurance Sector*, *BNM Guidelines on the Provision of Electronic Banking (e-banking) Services*, the *BNM Guidelines on Data Management and Management Information System (MIS) Framework for the Banking Sector* and the Securities Commission Malaysia's *Guidelines on Management of Cyber Risk*. These standards and guidelines will be further discussed below.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

No such issues have arisen thus far in Malaysia.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There are currently no applicable laws in Malaysia that generally require organisations to report information related to Incidents or potential Incidents to a regulatory or other authority.

However, in August 2018, the PDP Commissioner published the Public Consultation Paper (No. 1/2018) entitled "The Implementation of Data Breach Notification" (the "**DBN Public Consultation Paper**") which would be applicable to organisations who are required to register under the PDPA and who process personal data or have control over or authorise the processing of any personal data (i.e. registered data users under the PDPA).

Pursuant to the DBN Public Consultation Paper, the PDP Commissioner intends to implement a data breach notification mechanism ("**DBN**") in Malaysia, where data users are required to notify and inform the relevant authorities and affected parties when a data breach has occurred within the organisation. Organisations will be required to report on:

(i) details about the Incident, (i.e. summary of the event and circumstances, type and amount of personal data involved in the Incident and the estimated number of affected individuals);
(ii) the organisation's containment or control measures (i.e. details of actions/measures taken or to be taken to contain the breach and the potential harm of the breach, especially to the affected individuals);
(iii) details and requirements with regards to notification (i.e. identification of the persons who have been notified about the breach, details whether any regulatory bodies/law enforcement agencies have been notified about the breach, the method(s) used by the organisation to notify the affected individual about the Incident, any advice given to the affected individual, the requirement for the PDP Commissioner to be notified no later than 72 hours after having become aware of the breach); and

(iv) details on the organisations' training and guidance in relation to data protection (i.e. whether the organisation had provided training/awareness programmes to staff members prior to the Incident, whether the staff members involved in the Incident had received training in the last 24 months and whether the organisation had provided any detailed guidance to staff on the handling of personal data in relation to the reported Incident).

The DBN Public Consultation Paper in its current draft form merely provides that data users are to report to the authority and the affected/relevant parties where a breach has occurred in an organisation. However, the PDP Commissioner has not clarified the scope of such "breach" nor identified the events which would trigger reporting obligations, and whether any defences or exemptions exist by which the data subject might prevent publication of that information.

The DBN Public Consultation Paper is expected to come into force by the end of 2018.

Certain sector-specific guidelines have been issued imposing such requirements. Some examples are as follows:

- **Banking Sector:** *BNM's Guidelines on Management of IT Environment* ("**GPIS 1**") outline the minimum responsibilities and requirements for mitigating risks pertaining to the IT environment.

  Under the Guidelines, banks are required to report to BNM on any serious security breaches, system down-time and degradation in system performance that critically affects the bank/financial institution, immediately upon detection by providing "initial information/observation" and the subsequent formal report within two days; and
- **Capital Market:** *Securities Commission Malaysia's Guidelines on Management of Cyber Risk* sets out the roles and responsibilities of capital market entities, policies and procedures that should be developed and implemented, requirements for managing cyber risk and reporting requirements to the Securities Commission Malaysia. Under the said Guidelines, the capital market entities must report to the Securities Commission Malaysia on any detection of a cyber Incident impacting the entity's information assets or systems, on the same day of the Incident. The entities are also required to report any cyber breaches to the board of directors and periodically update the board on emerging cyber threats and their potential impact on the entity.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

While there are no general restrictions with regards to voluntary sharing of information pertaining to an Incident, this is subject to sector-specific regulations and regulatory oversight which may constrain an organisation from sharing such information. Additionally, where the information involves personal data, the organisation needs to make sure that the disclosure of the said personal data must fall within the exceptions under the PDPA.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

There are currently no general requirements under Applicable Laws for organisations to report information relating to Incidents or potential Incidents to affected individuals. Notwithstanding the foregoing, the DBN Public Consultation Paper (which is currently in the public consultation stage, and pending formal issuance as discussed in question 2.5 above) requires organisations to provide information in relation to:

(i) details of actions/measures taken or to be taken to contain the breach;

(ii) advice given to the affected individual; and

(iii) the potential harm of the breach on the affected individuals and the method(s) used by the organisation to notify affected individuals about the Incident.

Apart from the general requirement for data users to report on data breach events, the DBN Public Consultation Paper has not specified the circumstances (i.e. what constitutes a "data breach") in which this reporting obligation is triggered.

Further to the above, certain sector-specific guidelines require the applicable organisations to implement policies or procedures to inform the relevant stakeholders of the Incident (e.g. the *SC Guidelines on Management of Cyber Risk* requires the relevant entity to implement communication procedures that will be activated by the entity in the event of a cyber breach, which include reporting procedures, information to be reported, communication channels, list of internal and external stakeholders and a communication timeline).

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, they do not.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Regulators responsible for enforcing requirements are generally either sector-specific or subject matter-specific, including but not limited to:

Sector/Subject Matter	Relevant Statute/ Regulations	Regulator
Information Security/Network Reliability and Integrity	Communications and Multimedia Act 1998	Malaysian Communications and Multimedia Commission (MCMC)
Personal Data	Personal Data Protection Act 2010	Personal Data Protection Department/ Commissioner's Office
Penal Offences	Penal Code, Computer Crimes Act 1997	Royal Malaysian Police
Sector-Specific Regulations	Banking and Financial Sector Guidelines	Central Bank of Malaysia or Bank Negara Malaysia (BNM)
	Securities Commission Guidelines	Securities Commission Malaysia (SC)

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Penalties for failure to comply with any of the abovementioned

requirements are dependent upon the respective statutes, regulations or guidelines, for example:

- non-compliance with the PDPA may result in the organisation, upon conviction, to be liable to a maximum fine ranging from RM100,000 to RM500,000 or imprisonment ranging from one to three years, or both;
- non-compliance with the provisions under the CMA may result in the organisation, upon conviction, to be liable to a maximum fine ranging from RM50,000 to RM500,000 or imprisonment ranging from one to five years, or both;
- contravention of the provisions under the CCA or Penal Code would subject the organisation to enforcement by the Royal Malaysian Police, and may expose the organisation to liability involving a fine ranging from RM25,000 to RM150,000 or imprisonment of three to 10 years or both; or
- non-compliance with the relevant sector-specific guidelines may expose the organisation to enforcement actions by the relevant regulators (e.g. BNM or the SC), and may subject the organisation to regulatory sanctions such as a warning, public or private reprimands, an order to mitigate remedy the non-compliance, or even imposition of a monetary penalty. In cases involving severe non-compliance, the regulators may commence prosecution against the organisation.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

There are no reported cases in Malaysian law journals in relation to any non-compliance of the abovementioned requirements.

From the regulatory perspective, regulators may impose regulatory sanctions on their licensees. These regulatory sanctions may be issued either privately (e.g. BNM) or publicly (e.g. MCMC) by regulators, depending on the regulator.

A list of investigations and prosecutions is available on MCMC's official website.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

As stated in questions 2.3 and 2.5 above, apart from the PDP Standards which prescribe a list of minimum security standards to be complied with by data users, cybersecurity obligations and requirements vary across different sectors and are imposed in sector-specific legislation, regulations, standards and/or guidelines.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Financial services sector

Guidelines on Internet Insurance

The Guidelines state that an internet insurance system security arrangement should minimally achieve data privacy and confidentiality, data integrity, authentication, and non-repudiation and network and access controls. Insurers are required to put in place critical technologies and to have a thorough and documented security procedure in relation to the risk exposures and needs of its internet insurance, such as:

(a) the latest critical technologies available such as firewalls, intrusion detection systems, anti-virus or virus-protection, encryption, virtual private networks (VPNs), public key infrastructure (PKI) and payment protocols; and

(b) security procedures such as user IDs and passwords, time stamping, reconciliation of all transactions, segregation of roles and responsibilities, audit trails, and testing.

BNM Guidelines on the Provision of Electronic Banking (e-banking) Services

In the *Guidelines on E-Banking*, security standards to be applied are based on the risk management of different e-banking types. The Guidelines set out different minimum security standards for different types of banking services. For example, in transactional services which present the greatest risk in e-banking (as it links to the financial institutions' internal networks and computer systems that hold critical account information and other information assets), the Guidelines require utilisation of the highest level of protection including strong authentication and encrypted transmission of highly sensitive data.

Bank Negara Guidelines on Data Management and Management Information System (MIS) Framework

These Guidelines set out several principles and elaborate on the specific safeguards to be applied for each principle. Among the safeguards required are that banks/financial institutions are to obtain the MS ISO/IEC 27001 Information Security Management Systems (ISMS) certification for critical systems, particularly the payment and settlement systems, to ensure that safeguards and security measures implemented over data and IT systems are effective.

Telecommunications sector

There are currently no specific cybersecurity obligations imposed on licensees under the CMA. However, under section 263 of the CMA, the Commission or other authority, may make requests in writing to its licensees requesting the licensees to assist the Commission or any other authority, as far as reasonably necessary, in preventing the committing or attempted committing of an offence under any written law of Malaysia, or otherwise in enforcing the laws of Malaysia, including the protection of the public revenue and preservation of national security.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Failure by a company to prevent, mitigate, manage or respond to an Incident would potentially give rise to a breach of directors' duties.

In the event of any breach or non-compliance of statutory requirements by the organisation, the directors may also be held jointly or severally liable for such breach or non-compliance.

Under section 133 of the PDPA, it is expressly provided that the commission of any offence by the body corporate may also render the officers of the body corporate (e.g. directors, the chief executive officer, managers, etc., who were responsible for the management of the affairs of the body corporate) to be charged severally or jointly with the body corporate, and in such instances may also be found to have committed the offence.

Directors may also be found liable for such failure under the relevant sector-specific standards or guidelines. For example, in the banking

and financial sector, the *Guidelines on Data Management and MIS Framework* issued by BNM provide that senior management and the board of directors must play a key role in the development of a data management and management information system framework; and in capital markets sector, the *Guidelines on Management of Cyber Risk* issued by the SC set out the roles and responsibilities of the board of directors and management in the oversight and management of cyber risk. These provide that directors are subject to certain responsibilities and consequently may be held responsible for any non-compliance therewith.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There is no general requirement under Malaysian laws for companies to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments; and (d) perform penetration tests or vulnerability assessments. Requirements are generally sector-specific and in accordance with the relevant standards or guidelines (e.g. *SC Guidelines on Management of Cyber Risk* requires cyber risk policies and procedures to be implemented by the organisation, and sets out the required contents of such policies and procedures as well as an Incident response template).

Notwithstanding the above, the DBN Public Consultation Paper (which, as described in question 2.5 above, is still in the public consultation stage and pending official issuance by the PDP Commissioner) provides in general that a training/awareness programme and detailed guidance should be given to the organisation's staff for handling such Incidents.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Companies are not subject to general disclosure requirements in relation to cybersecurity risks or Incidents (whether to listing authorities, the market or otherwise in their annual reports).

Disclosure requirements in relation to cybersecurity risks or Incidents are sector-specific. For example, the *Guidelines on Management of Cyber Risk*, issued by the Securities Commission Malaysia, requires capital market entities to develop and implement cyber risk policies and procedures, which must include the strategy and measures to manage cyber risk encompassing prevention, detection and recovery from a cyber breach.

Notwithstanding the above, the DBN Public Consultation Paper (which, as described in question 2.5 above, is still in the public consultation stage and pending official issuance by the PDP Commissioner) provides in general that notification of Incidents must also be made to other regulatory bodies/law enforcement agencies.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Apart from the Applicable Laws (as set out at question 2.1 above), companies would also be subject to specific requirements in relation to cybersecurity under the relevant sector-specific standards or guidelines.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In the event of an Incident, the company or organisation may be subject to civil actions on grounds of breach of contract or breach of statutory duties under the Applicable Laws (as set out at question 2.1 above).

In order to bring a claim on grounds of breach of contract, the claiming party must establish that there was a contractual duty in respect of cybersecurity (e.g. duty to protect confidential information or personal data), that there was a breach of such duty, and the loss or damage occasioned by such breach. A breach of statutory duty in itself would give rise to a right to commence civil action, although the quantum of damages would be dependent on the extent of loss or damage suffered by the claiming party. The company or organisation may also be liable under tort, as set out in question 5.3 below.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

An example would be *Dynacraf Industries Sdn Bhd v Lee Kooi Khoon* [2008] 3 ILR 265, where an employer commenced action against a dismissed employee for alleged unauthorised interception and disclosure of electronic communication (in this case, another employee's private emails), in contravention with section 234 of the CMA (interception of communication). Apart from the foregoing, civil actions on grounds of copyright infringement, breach of confidence, have been brought in Malaysian courts.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

In the event of an Incident, the company or organisation may also potentially be exposed to tortious liability on grounds of negligence, as the aggrieved party may allege loss or damage as a result of the company's or organisation's breach of duty of care in relation to cybersecurity.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out cyber risk insurance against Incidents in Malaysia. Cyber risk insurance may either be first party coverage (i.e. to insure against loss and damage sustained by the insured, i.e. the organisation itself) or third-party coverage (i.e. to insure against liability for loss, damage or personal injury caused to a third person, namely the customers or clients of the organisation).

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no known regulatory limitations in respect of cyber risk insurance coverage. However, risk exposure due to the company's

or organisation's own negligence or wilful default will likely be excluded by the insurer from the scope of insurance policy coverage.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There are no specific requirements under the Applicable Laws requiring monitoring of employees and for the employees to be under an obligation to report cyber risks, security flaws, Incidents, etc. to the employer. However, sector-specific guidelines may prescribe that employees be made aware of and understand the cyber risk policies procedures, the possible impact of cyber threats, as well as their roles in managing such threats (*Guidelines on Management of Cyber Risk*, issued by the Securities Commission Malaysia).

Additionally, the DBN Public Consultation Paper (which, as described in question 2.5 above, is still in the public consultation stage and pending official issuance by the PDP Commissioner) provides in general that a training/awareness programme and detailed guidance should be given to the organisation's staff for handling such Incidents.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no known Applicable Laws that may prohibit or limit the reporting of cyber risks, security flaws, Incidents by an employee, etc. In fact, the Whistleblower Protection Act 2010 ("**WPA**") was passed to encourage and facilitate the disclosures of improper conduct of companies or organisations by protecting the informants making such disclosures. It is further provided under section 6(5) of the WPA that any provision in any contract of employment which purports to preclude the employee from making a disclosure of improper conduct shall be to that extent void.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Royal Malaysian Police, the MCMC and other relevant regulatory authorities are granted wide investigatory powers under the relevant statutes (as set out in question 2.9 above).

In general, the law enforcement or regulatory authorities are authorised under the relevant statutes to exercise the following investigatory powers during an investigation:

- the power to investigate the relevant persons;
- search and seizure, by warrant or without warrant;
- request for access to computerised data;
- the power to intercept communications;
- the power to require the production of records, accounts, computerised data, documents, etc., and to make such inquiry as may be necessary to ascertain if the relevant statutory provisions have been complied with;
- the power to require attendance of persons acquainted with the case;
- examination of persons acquainted with the case; and
- the power to institute prosecution, with consent in writing of the Public Prosecutor.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

While there are no legal requirements under the Applicable Laws for organisations to implement backdoors in IT systems specifically for law enforcement authorities, several cybersecurity-related statutes provide the need for law enforcement authorities to be provided with the relevant encryption keys, passwords, decryption codes, software or hardware or any other means required in order to have access to computerised data during the course of investigations (section 249 of the CMA; section 10 of the CCA).

Deepak Pillai
Christopher & Lee Ong
Level 22 Axiata Tower
No. 9 Jalan Stesen, Sentral 5
Kuala Lumpur Sentral, 50470
Kuala Lumpur
Malaysia

Tel: +603 2267 2675
Email: deepak.pillai@christopherleeong.com
URL: www.christopherleeong.com

Deepak has practised exclusively in the areas of Telecommunications & Technology law and Personal Data Protection for two decades and is acknowledged as a leading Telecommunications & Technology lawyer in Malaysia.

Deepak advises clients on matters relating to IT contracts, electronic commerce, online financial services, outsourcing, telecommunications, IT security, personal data protection and digital media. He advises a wide array of international, private and public sector clientele in addressing the commercial, regulatory and policy issues relating to information and communications technology law, ranging from negotiating complex information technology contracts to advising public sector agencies on proposed technology related legislation and policies.

Described in *The Legal 500* over the years as "*the most recognised IT specialist in Malaysia*", and "*pioneering the practice of IT law as a discrete area of law in Malaysia*".

Deepak has been listed by the *Asia Pacific Legal 500* as a leading individual in the area of IT and Telecommunications from 2001 to date.

Yong Shih Han
Christopher & Lee Ong
Level 22 Axiata Tower
No. 9 Jalan Stesen, Sentral 5
Kuala Lumpur Sentral, 50470
Kuala Lumpur
Malaysia

Tel: +603 2267 2715
Email: shih.han.yong@christopherleeong.com
URL: www.christopherleeong.com

Shih Han practices exclusively in the areas of Technology, Media and Telecommunications (TMT), and Data Protection. Prior to joining the firm, she was a dispute resolution associate in a reputable firm handling primarily civil and corporate litigation matters. Since joining the firm and making the transition to corporate practice, she has been involved in the areas of corporate commercial, mergers & acquisitions, and general corporate advisory. She currently focuses on the areas of technology, media, telecommunications and data protection, with information security and data protection being her specialised area.

She now regularly advises clients on matters relating to information and communications technology, information security and data protection, telecommunications, and media and advertising laws. This ranges from the preparation and drafting of technology-related contracts and policies to advising clients on matters potentially leading to dispute resolution. She also regularly advises clients on technology- and media-related regulatory and compliance matters.

CHRISTOPHER & LEE ONG

Christopher & Lee Ong ("CLO") is one of Malaysia's established and respected law firms, providing high-quality advice to clients across the commercial spectrum, with extensive experience in handling complex deals and disputes involving large local and multinational corporations, and governments and their agencies, as well as smaller local enterprises.

CLO's technology, media & telecommunications ("TMT") practice group is one of the most established and respected practices in the Asia Pacific region. With clients ranging from state governments and statutory boards to multinational corporations in the telecommunications, computer hardware and software sectors, the firm has been involved in many of the largest and most complex IT and telecommunications projects in recent years. The firm regularly advises clients on matters relating to IT contracts, electronic and mobile commerce, online financial services, outsourcing, telecommunications, cybersecurity, personal data protection, as well as regulatory and policy issues relating to information and communications technology law.

The firm's TMT practice group was recently awarded the *Technology, Media and Telecommunications Law Firm of the Year 2017* by *Asian Legal Business* at the Malaysian Law Awards 2017.

Mexico

Creel, García-Cuéllar, Aiza y Enríquez, S.C.

Begoña Cancino

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

There is no definition in Mexican law of the terms "cybercrime" and "cybersecurity"; however, the Federal Criminal Code regulates illegal behaviours committed through electronic means that could be identified as cybercrimes by the use of electronic means for their commission.

Regarding examples of jurisdiction in Mexico, according to Article 16 of the Political Constitution of the United Mexican States ("Mexican Constitution"), no one shall be disturbed in his/her private affairs, family, home, papers or possessions (including private information), except by written order of a competent authority, duly grounded in law and fact, which sets forth the legal cause of the proceeding. In this regard, any non-consented access to private information may be sanctioned by law; thus, only a federal judicial authority may authorise any investigation regarding criminal offences.

Hacking (i.e. unauthorised access)

Article 211*bis* of the Federal Criminal Code provides that whoever, without authorisation, modifies, destroys or causes loss of information contained in systems or computer equipment protected by a security mechanism shall be imposed with a prison sentence of six months to two years, by the relevant authority, as well as a fine of approximately MN$8,004.00 to MN$24,012.00. The aforementioned penalty could be duplicated in case the information is used for one's own benefit or to benefit a third party.

Denial-of-service attacks

The Federal Criminal Code does not provide any definition, or similar definition, for this criminal offence.

Phishing

The Federal Criminal Code does not provide any definition for phishing; however, such criminal offence could be considered as fraud. According to Article 386 of the Federal Criminal Code, a person commits fraud when he/she, with the intent of obtaining a financial gain, handles information through deceit, takes advantage of errors, or misleads a person.

In such case, the relevant authority shall impose a prison sentence of three days to 12 years, as well as a fine of approximately MN$2,400.00 to MN$24,012.00, depending on the value in each case.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

The Federal Criminal Code does not provide any definition for this criminal offence; however, this type of behaviour is similar to hacking. The aforementioned penalties are applicable in this case.

In case the criminal offence is committed against the state, the relevant authority shall impose a prison sentence of one to four years, as well as a fine of approximately MN$16,000.00 to MN$48,024.00.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

The Federal Criminal Code provides this criminal offence as "hacking", which is described above.

Identity theft or identity fraud (e.g. in connection with access devices)

The Credit Institutions Law provides that a person who produces, manufactures, reproduces, copies, prints, sells, trades or alters any credit card, debit card, cheques or, in general, any other payment instrument, including electronic devices, issued by credit institutions, without authorisation of the holder, shall be imposed a prison sentence of three to nine years, by the relevant authority, as well as a fine of approximately MN$2,401,200.00 to MN$24,012,000.00.

In addition, the Federal Criminal Code provides that a person who, with or without authorisation, modifies, destroys or causes loss of information contained in credit institutions' systems or computer equipment protected by a security mechanism shall be imposed with a prison sentence of six months to four years, by the relevant authority, as well as a fine of approximately MN$8,004.00 to MN$24,012.00.

Moreover, a person who without authorisation knows or copies information in credit institutions' computer systems or equipment protected by a security mechanism shall be imposed a prison sentence of three months to two years, as well as a fine of approximately MN$4,002.00 to MN$24,012.00.

All the penalties aforementioned could be duplicated if the criminal offence is committed by any counsellor, official, employee or service provider of any credit institution.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

As mentioned, the Credit Institutions Law provides that any person who produces, manufactures, reproduces, copies, prints, sells, trades or alters, any credit card, debit card, cheque or, in general, any other payment instrument, including electronic devices, issued by credit institutions, without authorisation of the holder, shall be imposed with a prison sentence of three to nine years, as well as a fine of approximately MN$2,401,200.00 to MN$24,012,000.00. The

aforementioned penalties may be duplicated if the criminal offence is committed by any counsellor, official, employee or service provider of any credit institution.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Yes: espionage; conspiracy; crimes against means of communication; tapping of communications; acts of corruption; extortion; and money laundering could be considered as threats to the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

Failure by an organisation to implement cybersecurity measures

Considering the absence of a specific law which regulates cybersecurity in Mexico, there are no minimum protective measures that organisations must implement to protect data and information technology systems from cyber threats; however, the Federal Law on Protection of Personal Data held by Private Parties ("Data Protection Law") provides that data controllers have to implement diverse technical, physical and organisational measures in order to protect information against damage, loss, alteration, destruction, use, or unauthorised access or processing.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes; however, Mexico has not yet adopted international standards related to cybersecurity.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Yes, in the following cases:

1) The Federal Law Against Organized Crime provides: (a) that in the investigation of a crime in which it is assumed on good grounds that a member of organised crime is involved, it is possible to tap private communications; and (b) the obligation of concessionaires, authorised entities and any person holding a means or system that could be intercepted, to cooperate with the authorities, prior to a judicial order.
2) The General Law to Prevent and Sanction Kidnapping Crimes provides the possibility to intercept private communications.
3) The National Security Law, in case of an immediate threat to national security, provides that the Mexican government must request a judicial warrant to intercept private communications for national security purposes.
4) The Federal Telecommunications and Broadcasting Law ("FTBL"), according to Articles 189 and 190, provides that: (i) concessionaires; (ii) authorised entities; and (iii) service providers of applications or contents, are required to: a) allow the corresponding competent authorities to control and tap private communications; and b) provide the support that such authorities request, in terms of the applicable law.

In addition to the federal legislation provided above, there are state laws that allow the interception of individual communications prior to any request from the relevant state authorities (Public Prosecutor of the corresponding state) to a federal judge.

Intervention of private communications is not allowed in: electoral tax; commercial; civil; labour; or administrative matters, or in the case of communications between the arrested and his/her counsel.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

As mentioned, the Federal Criminal Code also regulates as a criminal offence the act of sabotage or unlawful interference with: roads, public services, or state services; steel, electric or basic industries; and centres of production or distribution of weapons, ammunition or military equipment, with the aim of disrupting the economic life of the country or to affect its ability to defend itself.

Also, the relevant Code protects means of communication such as telegrams, telephone lines, radio communications, telecommunication networks, and any component of an installation of production of magnetic or electromagnetic energy or its means of transmission.

In addition, the Federal Criminal Code provides that persons who manufacture, import, sell or lease any device or system, or commit any act with the purpose of decoding any encrypted/protected satellite signal without the legitimate authorisation of the licensed distributor, shall be imposed with a prison sentence of six months to four years.

On the other hand, the Law on Negotiable Instruments and Credit Operations sanctions diverse actions that affect any kind of financial payment instrument (e.g., credit or service cards) or the information contained on them.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

- The Mexican Constitution.
- The FTBL.
- The Data Protection Law, its Regulations, Recommendations, Guidelines and similar regulations on data protection.
- The Federal Law on Transparency and Access to Public Information.
- The General Law on Transparency and Access to Public Information.
- General Standards as the Mexican Official Standard Regarding the Requirements that shall be Observed when Keeping Data Messages.
- The Law on Negotiable Instruments and Credit Operations.
- The Mexican Federal Tax Code.
- The Credit Institutions Law.
- The Sole Circular for Banks.
- The Industrial Property Law.
- The Mexican Copyright Law.
- The Federal Criminal Code.
- The National Security Law.
- The Federal Labour Law.
- The Federal Law for the Federal Police.
- The National Development Plan 2013–2018.

- The National Programme of Public Security 2014–2018.
- The National Programme of Security 2014–2018.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

This is not applicable in Mexico.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

As mentioned, there are no minimum protective measures that organisations must implement to protect data and information technology systems from cyber threats; however, the Data Privacy Law provides that data controllers have to implement diverse technical, physical and organisational measures in order to protect information against damage, loss, alteration, destruction, use, or unauthorised access or processing.

In addition to the foregoing, there are certain specific mandatory security measures that certain industries must adopt to protect their customers' data. Banking laws and regulations provide that banks must implement certain security measures in electronic banking transactions and require the use of several passwords depending on the amount and nature of the transaction.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

This is not applicable in Mexico.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There is no obligation to report Incidents or potential Incidents to the authorities; however, the General Law on Transparency and Public Information Access provides, in Article 70 Section XLVII, that authorities must provide access and keep updated, for statistical purposes, the list of requests made to telecommunications concessionaires, service providers or Internet applications related to the interception of private communications, access to the registry of communications, and the real-time geo-location of communication equipment, that contains the object, temporary scope and legal grounds of the request and, if applicable, a statement of judicial authorisation.

On the other hand, Data Privacy Laws do not provide a penalty for failure to comply with the rules on reporting threats or breaches; nevertheless, the National Institute for Access to Public Information and Data Protection ("INAI") is empowered to evaluate if the cause that originated a data breach was caused by a failure of compliance or negligence.

By the interpretation of the Mexican Constitution, organisations must cooperate with government agencies regarding Incidents; however, no law establishes specific requirements to report Incidents or potential Incidents.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Please refer to our answer in question 2.5.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

There is no obligation to report any Incidents or potential Incidents; however, Data Protection Law provides that security breaches that materially affect the property or moral rights of data owners will be reported immediately by the data controller to the data owner, so that the latter can take appropriate action to defend its rights.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, the responses to questions 2.5 to 2.7 do not change.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The INAI is in charge of: (i) guaranteeing people's right of access to public government information; (ii) protecting personal data in possession of the federal government and individuals; and (iii) resolving denials of access to information that the dependencies or entities of the federal government have formulated.

The Federal Telecommunications Institute ("IFT") is in charge of regulating telecommunications and broadcasting services.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The Applicable Laws are silent in this regard.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

This is not applicable in Mexico.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes. According to the Data Protection Law, the data controllers have to implement diverse technical, physical and organisational measures in order to protect information against damage, loss, alteration, destruction, use, or unauthorised access or processing.

On the other hand, the Federal Criminal Code and the Law on Negotiable Instruments and Credit Operations provide several sanctions in order to avoid criminal offences regarding cybersecurity.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes. Regarding financial services, the Law on Negotiable Instruments and Credit Operations and the Credit Institutions Law, including the Federal Criminal Code, are applicable in order to avoid cybercrimes.

The FTBL and the Federal Criminal Code are applicable in this matter.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

There are no specific laws in Mexico related to cybersecurity responsibilities or liabilities of personnel and directors. Nevertheless, and in accordance with the Data Protection Law, every private party, individual or organisation that processes personal information (data controller), has the obligation to appoint a data person or department (data protection officer) who will be a representative for the organisation in privacy and data protection matters and in charge, within the organisation, of the correct processing of personal data (including verification of security measures), as well as of processing requests from data owners for the exercise of their rights to access, rectification, suppression or rejection.

In relation to information security, data protection officers shall adopt measures to guarantee due processing of personal data, privileging the interests of the data owners and their reasonable expectation of privacy.

The measures that the data protection officer shall adopt, and that may be related to cybersecurity, include the following: (i) issuing policies and programmes, which shall be mandatory within the organisation; (ii) implementing training programmes; (iii) implementing a monitoring and surveillance system and internal or external audits to verify compliance with privacy policies; (iv) assigning resources for the implementation of programmes and policies related to privacy; (v) implementing a risk-detection programme to identify privacy risks when launching new products, services, technologies and business models as well as risk-mitigation strategies; (vi) periodically reviewing security policies and programmes to determine whether amendments are needed; (vii) performing compliance checks; and (viii) implementing personal data-tracking systems to trace which data are collected and where they are stored.

The Data Protection Law does not provide a specific sanction for data protection officers, responsible personnel and directors.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Regarding personal data, all data controllers must designate a data protection officer or department; however, the Applicable Laws are silent on cybersecurity matters.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

The Applicable Laws are silent in this regard.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

The Applicable Laws are silent in this regard.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

According to Article 32 of the Federal Criminal Code, organisations and companies are civilly liable for the damages caused to third parties by crimes committed by their partners, managers and directors. The state is similarly liable for the crimes committed by its public officials.

The Federal Civil Code provides a standard of civil liability established in Article 1910, which provides that a party that illegally causes harm to another person shall be obliged to repair the damage, unless he/she proves that the damage was produced as a consequence of the victim's guilt or negligence.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

This is not applicable in Mexico.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

This is not applicable in Mexico.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents in our jurisdiction.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

This is not applicable in Mexico.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There are no specific requirements; however, the Data Protection Law provides that a person who is involved with personal data is obligated to establish and maintain physical and technical administrative security measures and in case of any breach, such employee must notify the data protection officer.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

This is not applicable in Mexico.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Applicable Laws empower the following authorities to investigate an Incident: (i) the General Attorney Office; (ii) Public Prosecutors; (iii) the INAI; and (iv) the IFT.

Public Prosecutors in Mexico are in charge of investigating and resolving cyber activities; a cyber police service has been created to follow up on crimes or unlawful activities committed through the Internet. Complaints directed to the cyber police can be submitted via its website, by phone, or through a Twitter or email account; in addition, the Federal Police have created a scientific division called the National Centre For Cyber-Incidents Response, specialised in providing assistance to the victims or claimants of cyber threats and cyber attacks.

In the case of data protection, the INAI may conduct investigations to follow up personal data matters. The IFT is in charge of the telecommunications sector.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

The Applicable Laws are silent in this regard.

Begoña Cancino
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Torre Virreyes
Pedregal 24, 24th Floor
Molino del Rey
11040, Mexico City
Mexico

Tel: *+52 55 4748 0679*
Email: *begona.cancino@creel.mx*
URL: *www.creel.mx*

Begoña Cancino is a partner in the Mexico City office. Her practice focuses on Intellectual Property, Data Privacy, Regulatory and Administrative Litigation. From the standard IP front, Ms. Cancino counsels clients from all kinds of industries with the protection and enforcement of their IP rights in Mexico, assisting also with the transfer of IP portfolios within the context of complex corporate transactions involving all sort of IP rights (such as trademarks, copyrights and appellations of origin). Ms. Cancino also provides assistance with her legal advice on regulatory and advertising, assessing her clients to comply with all applicable provisions with COFEPRIS and PROFECO. She has represented clients in all sorts of administrative litigation proceedings, in general concerning advertising, health, environmental and, of course, IP matters, before administrative authorities and federal judicial courts. Pursuant to the data privacy aspects of her practice, Ms. Cancino has counselled clients from multiple industries in the drafting and implementation of internal policies, privacy notices and specific legal concerns, not only regarding client daily operations, but also within the context of cross-border transactions and internal investigations for compliance.

CREEL GARCÍA-CUÉLLAR AIZA Y ENRÍQUEZ

Creel, García-Cuéllar, Aiza y Enríquez is an award-winning, full-service corporate law firm. It has over 80 years of experience in providing international and domestic clients with technical excellence, knowledge of the market and unparalleled client service. The firm is a strategic service provider to clients with the most complex and demanding transactions and projects, affording them certainty and peace of mind. The firm provides innovative solutions to many of the largest, most intricate, first-ever market-leading deals in Mexico. We are a full-service corporate law firm, specialising in the following practice areas and industries: antitrust and competition; arbitration and dispute resolution; banking and finance; bankruptcy and restructuring; capital markets; corporate and commercial; employment and labour; energy and natural resources; environmental; infrastructure; insurance and reinsurance; intellectual property; mergers and acquisitions; private equity; *pro bono*; project development and finance; real estate; social security; tax; telecommunications; and transportation.

Nigeria

Ijeoma Uju

Templars

Ijeamaka Nzekwe

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes. The Cybercrimes (Prohibition and Prevention etc. 2015) Act (the "Cybercrimes Act") makes it an offence for any person, without authorisation, to intentionally access in whole or in part a computer system or network with the intent of obtaining computer data, securing access to any program and commercial or industrial secrets or classified information.

Maximum penalty: imprisonment for a term of not more than seven years or a fine of not more than N7,000,000.00, or both such fine and imprisonment.

In June 2018, a suspected fraudster was arraigned before a Lagos Magistrate's Court for allegedly conniving with another suspect, to hack into the mobile app account of Eco Bank Plc and unlawfully withdrawing the sum of N207,000,000.00.

Denial-of-service attacks

Denial-of-service is covered by section 8 of the Cybercrimes Act, which makes it an offence for any person to intentionally commit an act without lawful authority which causes the serious hindering of the functioning of a computer system by inputting data which prevents the computer system from functioning in accordance with its intended purpose.

Maximum penalty: imprisonment for a term of not more than two years or a fine of not more than N5,000,000.00, or both such fine and imprisonment.

Phishing

Under the Cybercrimes Act, anyone who attempts to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication through emails or instant messaging either in the form of an email from what appears to be your bank asking a user to change his or her password or by revealing his or her identity so that such information can later be used to defraud the use, is liable to three years' imprisonment or a fine of N1,000,000.00, or both.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. The Cybercrimes Act makes it an offence for any person to engage in malicious or deliberate spread of viruses or any malware thereby causing damage to critical information in public, private or financial institution's computers. Such a person is liable to three years' imprisonment or a fine of N1,000,000.00, or both.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Under the Cybercrimes Act, it is an offence for any person who, with intent to commit an offence under the Act, has in his possession any device, including a computer program, a computer password, access code or similar data by which a computer system or network is capable of being accessed for the purpose of committing an offence under the Act.

Maximum penalty: imprisonment for a term of not more than two years or a fine of not more than N5,000,000.00, or both such fine and imprisonment.

Identity theft or identity fraud (e.g. in connection with access devices)

The Cybercrimes Act provides that any person who is engaged in the services of any financial institution, and as a result of his special knowledge commits identity theft of its employer, staff, service providers and consultants with the intent to defraud is guilty of an offence and upon conviction shall be sentenced to seven years' imprisonment or a fine of N5,000,000.00, or both.

On August 1, 2018 the EFCC (Kaduna Branch) secured the conviction of one accused on a charge bordering on impersonation, forgery and obtaining by false pretence.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

The Cybercrimes Act makes it an offence for any person employed by or under the authority of any bank or other financial institutions to divert electronic mails with intent to defraud.

Maximum penalty: imprisonment for a term of not more than five years or a fine of not more than N7,000,000.00, or both such fine and imprisonment.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Other activities include:

1. Child pornography: the maximum punishment is imprisonment for a term of 10 years or a fine of not more than N20,000,000.00, or both such fine and imprisonment.
2. Cyberstalking: the maximum punishment is a fine of not more than N7,000,000.00 or imprisonment for a term of not more than three years, or both such fine and imprisonment.
3. Cybersquatting: the maximum punishment is imprisonment for a term of not more than two years or a fine of not more than

N5,000,000.00, or both such fine and imprisonment. The court may also make an order directing the offender to relinquish such registered name, mark, trademark, domain name, or other word or phrase to the rightful owner.

4. Racist and xenophobic offences: the maximum penalty is imprisonment for a term of not more than five years or a fine of not more than N10,000,000.00, or both such fine and imprisonment.
5. Importation and fabrication of E-Tools: the maximum penalty is imprisonment for a term of not more than three years or a fine of not more than N7,000,000.00, or both.
6. Breach of confidence by service providers: the maximum punishment is a fine of N5,000,000.00 and forfeiture of further equivalent of the monetary value of the loss sustained by the consumer.
7. Manipulation of ATM/POS terminals: the maximum penalty is five years' imprisonment or a fine of N5,000,000.00, or both.

Failure by an organisation to implement cybersecurity measures

Yes. The Advance Fee Fraud Act ("the AFF Act") provides that a failure of providers of any internet services to register with the Economic and Financial Crimes Commission ("EFCC") is an offence and is liable on conviction to imprisonment for a term of not less than three years without an option of a fine, and in the case of a continuing offence, a fine of N50,000 for each day the offence persists.

The Cybercrimes Act provides that any person or institution who fails to report an Incident to the National Computer Emergency Response Team ("CERT") within seven days of its occurrence commits an offence and will be liable to denial of internet services, in addition to payment of a mandatory fine of N2,000,000.00.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, the offences under the Act have extraterritorial application.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

No, there are no actions that might mitigate any penalty or constitute an exception to the above offences.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Yes, there are. The AFF Act provides that a person who is in possession of a document containing a false pretence commits an offence if he knows or ought to know, having regard to the circumstances of the case, that the document contains the false pretence. "Document" is defined under the Act to include a document transmitted through an electronic or electrical device.

Also, Section 5 of the Terrorism Prevention Act 2011 (as amended) (the "TPA") provides that any person who knowingly, in any manner, directly or indirectly solicits or renders support for the commission of an act of terrorism or to a terrorist group, commits an offence and is liable on conviction to imprisonment for a term of not less than 20 years. Support is defined to include incitement to commit a terrorist act through the internet, or any electronic means.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

1. The Cybercrimes (Prohibition and Prevention etc.) Act 2015.
2. The Advance Fee Fraud and other Related Offences Act 2006.
3. The Terrorism Prevention Act 2011, as amended.
4. The NCC Guidelines for Internet Service Providers.
5. Draft Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers 2018.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Yes. The Cyber Crimes Act provides that any person who, being employed by or under a Local Government of Nigeria, private organisation or financial institution with respect to working with any critical infrastructure, electronic mails, commits any act which he is not authorised to do by virtue of his contract of service or intentionally permits tampering with such computer, is guilty of an offence and is liable to a fine of N2,000,000.00 or imprisonment for three years.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. Under the AFF Act, in order to prevent cyber fraud, any person or entity providing an electronic communication service or remote computing service either by e-mail or any other form is required to: obtain from the customer or subscriber his full names; residential address, in the case of an individual; and corporate address, in the case of corporate bodies.

The NCC Guidelines for Internet Service Providers Guidelines (the "NCC Guidelines") also provide that Internet Service Providers ("ISPs") must ensure that users are informed of any statements of cybercrime prevention or acceptable internet use published by the Commission or any other authority, and that failure to comply with these acceptable use requirements may lead to criminal prosecution.

The NCC Guidelines also provide that ISPs must take reasonable steps to: inform users regarding proper email practices; ensure that users are updated regarding any changes to applicable laws or regulation; inform users of the consequences of acting contrary to proper email practices; and inform users of methods of reducing unsolicited email, including the availability of SPAM filters or similar services and the ISP's SPAM reporting and complaints procedures.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

We are not aware of any conflict of laws issues.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes. The Cybercrimes Act provides that any person or institution, who operates a computer system or a network, whether public or private, must immediately inform the (CERT) Coordination Center of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network, so that the national CERT can take the necessary measures to tackle the issues.

Also, if an ISP receives notification that any of its services have been used for the transmission of unsolicited communications contrary to these Guidelines, including the transmission of SPAM email, the ISP is required to take reasonable steps to notify the responsible user and describe the prohibited activity. If the prohibited activity is ongoing or serious, the ISP shall suspend or terminate the user's account (as provided for in paragraph 7 of the above), and shall report the activity to any responsible regulatory or law enforcement agency.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

The Applicable Laws do not restrict organisations from sharing information related to Incidents.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

There are no requirements under Applicable Laws to report information related to Incidents or potential Incidents to affected individuals.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, the responses do not change.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Nigerian Communications Commission (the "NCC") is responsible for enforcing the provisions of the Guidelines for the Provision of Internet Service.

The National Security Adviser ("NSA") is responsible for maintaining the (CERT) Coordination Center responsible for managing cyber Incidents in Nigeria.

The Attorney General of the Federation ("the AGF") supervises the implementation of the Cybercrimes Act, whilst law enforcement agencies are responsible for enforcing the provisions of the Cybercrimes Act and the TPA.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The AFF Act makes it an offence punishable with a fine of N100,000 and forfeiture of the equipment or facility used in providing the service for any person or entity providing electronic communication service or remote computing service to fail to obtain the stipulated details from its customer or subscriber.

The penalty under the Cybercrimes Act is stated in question 1.1 above.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

We are not aware of any enforcement action taken in cases of non-compliance with the above-mentioned requirements.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

No, market practice does not vary across different business sectors.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

(a) In the financial services sector: the Central Bank of Nigeria (the "CBN") recently issued a draft Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers (the "Draft DMB Guidelines").

The Draft DMB Guidelines provide for several specific legal requirements including: establishment of an information security steering committee by Deposit Money Banks ("DMBs") and Payment Service Providers ("PSPs") that shall be responsible for the governance of their cybersecurity programme; periodic review by the Compliance Department of DMBs and PSPs of their cybersecurity programmes and processes; and internal audit of DMBs/PSPs' cybersecurity programmes by an internal audit unit.

The Cybercrimes Act also requires financial institutions to verify the identity of its customers carrying out electronic financial transactions by requiring the customers to present documents bearing their names, addresses and other relevant information before the issuance of ATM cards, credit cards, debit cards and other related electronic devices.

(b) In respect of the telecommunications sector, the NCC Guidelines also require ISPs to ensure that users are informed of any statements of cybercrime prevention or acceptable internet use published by the Commission or any other authority, and that failure to comply with these acceptable use requirements may lead to criminal prosecution.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

There are no specific circumstances provided by the Applicable Laws whereby failure by a company to prevent, mitigate, manage or respond to an Incident amounts to a breach of directors' duties. However, every director owes a duty to exercise a degree of care, diligence and skill which a reasonable director would exercise. Hence, a failure to prevent or mitigate an Incident by a company may amount to a breach of duty by a director of the company if the director had not taken reasonable steps to prevent such Incident.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The Draft DMB Guidelines provide that DMBs/PSPs must:

- appoint a CISO;
- ensure consistent conduct of risk assessments, vulnerability assessments and threat analysis to detect and evaluate risk to the DMB/PSP's information assets and determine the appropriateness of security controls in managing risk; and
- update cyber risk assessments regularly to address changes or introduction of new technologies, products, etc., before deployment to ensure accurate risk measurement.

The Guidelines also require DMBs and PSPs to develop an Incident response policy with stakeholders which will stipulate, among others, the creation of a cyber Incident response plan.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

See the response in question 2.5.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, companies are not subject to other specific requirements under Applicable Laws except to the extent that the draft DMB Guidelines make specific provisions for DMBs and PSPs.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The Applicable Laws do not make any specific provision for civil actions that may be brought in relation to an Incident. However, a victim could institute an action in court in respect of a civil wrong done to him simultaneously with or after a criminal action and the court may in its discretion grant civil remedies to the victim in respect of the Incident. The civil action to be instituted will be determined by the nature of the Incident that has been committed. For example, where a contractual relationship exists, the victim of the Incident could prove breach of contract or negligence to claim relief from the courts. For example, the draft DMB Guidelines provide for the minimum baseline security measures to be put in place by DMBs and PSPs. Where an Incident results from non-adherence to the provisions of the Guidelines by DMBs and PSPs (when the guidelines are eventually issued), the victim who has incurred damage or loss may bring a civil action on the ground of the implied duty of care owed by the DMBs/PSPs.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

See our responses to question 1.1 above.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Depending on the nature of the Incident, there is potential liability in tort.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

There are no laws prohibiting organisations from taking out insurance against Incidents in Nigeria.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Currently, there are no regulatory limitations to insurance coverage against specific types of loss under Nigerian law.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The Cyber Crime Act has no direct provision or requirement in relation to the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents. In the same vein, there are no direct requirements for the reporting of cyber risk, security flaws, Incidents or potential Incidents by employees to their employer.

However, we note that the draft DMB Guidelines stipulate that the management of DMBs and PSPs is obligated to conduct background checks on employees who implement policies, and conduct procedures used to protect sensitive information of the DMBs and PSPs as part of the risk management steps.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no such Applicable Laws in this regard.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

For the purposes of a criminal investigation or proceeding, the Cybercrimes Act makes provision for a Judge to order a service provider to intercept, collect or record content data or traffic data associated with specified communications transmitted by means of a computer system where there are reasonable grounds to suspect that the content of such electronic communication is reasonably required. Further, the Cybercrimes Act makes provision for the Judge to authorise a law enforcement officer to collect or record such data through the application of technical means.

A law enforcement officer may apply *ex parte* to a Judge in chambers for the issuance of a warrant for the purpose of obtaining electronic evidence in a crime investigation in relation to Incidents.

Section 24 provides that the NSA or the Inspector General of Police ("IGP") may apply to the court for the issuance of a warrant for the purposes of a terrorism investigation. Such warrant may authorise the NSA or the IGP to enter any premises, and search and seize any relevant materials found in such premises.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no such requirements under Applicable Laws.

Ijeoma Uju
Templars
5th Floor, Octagon Building
13A, A.J. Marinho Drive
Victoria Island, Lagos
Nigeria

Tel: +234 1 4611 294
Fax: +234 1 2712 810
Email: ijeoma.uju@templars-law.com
URL: www.templars-law.com

Ijeoma is a Partner in the Corporate and Commercial practice group. She has over a decade of experience advising clients on day-to-day compliance requirements applicable to the operation of their businesses in various issues, including oil and gas, power, telecommunications, intellectual property, manufacturing, consumer protection, acquisition, sale of property, and labour and employment.

She advises clients on Nigerian law and policy affecting the regulation and operation of businesses in Nigeria, including the establishment of foreign businesses, corporate restructuring, mergers and acquisitions and relations with relevant regulatory authorities.

Ijeoma advises clients on intellectual property exploitation rights, registration, management and assignment/transfer of brands and counterfeiting. She provides advice on trademark and patent infringement rectification processes and jurisdictional constraints and prospects.

Ijeoma also manages the government relations aspect of clients' regulatory compliance, and has led various negotiations and/or engagements undertaken by the firm in this regard.

Ijeamaka Nzekwe
Templars
5th Floor, Octagon Building
13A, A.J. Marinho Drive
Victoria Island, Lagos
Nigeria

Tel: +234 1 279 9396
Fax: +234 1 2712 810
Email: ijeamaka.nzekwe@templars-law.com
URL: www.templars-law.com

Ijeamaka is an Associate in the Corporate and Commercial Group. She graduated from the Obafemi Awolowo University with First Class Honours where she achieved distinctions in commercial law, international law and the law of taxation.

Ijeamaka has gathered myriad of experiences across the different practice areas at the Firm. Particularly she has advised on issues relating to Banking and different financing structures, capital markets, corporate insolvency, mergers and acquisitions, projects and infrastructure, real estate, divestments, foreign direct investments, legal due diligence, regulatory compliance, dispute resolution, business development and general corporate and commercial matters.

Ijeamaka also advises clients on issues relating to the setting up of businesses in Nigeria, labour and industrial relations, as well as Nigerian law and policy affecting the operation of businesses, the establishment of foreign businesses and foreign investments in Nigeria. She also provides corporate governance and compliance advice to clients in connection with local and international transactions.

TEMPLARS

Templars is one of Nigeria's foremost integrated full-service commercial law firms. With offices in key commercial centres, the firm is strategically placed to offer quality legal services to clients across the length and breadth of the country.

At Templars, our strengths lie in our coverage of diverse legal fields, as well as our familiarity with the major sectors of the Nigerian economy. Not only are we well acquainted with domestic and international business transactions, typically involving strategic alliances and complex business arrangements; our lawyers work daily with all kinds and sizes of businesses, to structure, negotiate and document their transactions. We have built a reputation for understanding each client's peculiar business needs, and applying legal principles to craft workable solutions to meet those business objectives. We analyse the risks involved in our clients' transactions, and devise appropriate risk management formulae to assist in the mitigation and hedging of those risks.

At Templars we are always consistent with our commercial approach in the service of our clients, and we constantly employ cost-effective procedures in the pursuit of each mandate.

Norway

Christopher Sparre-Enger Clausen

Advokatfirmaet Thommessen AS

Uros Tosinovic

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Note: We have provided examples of prosecutions of the below activities in question 5.2 below.

Hacking (i.e. unauthorised access)

Forced entry into data systems and access to data systems by unauthorised means, including hacking, is regarded as a criminal offence under Section 204 of the Norwegian Penal Code of 20 May 2005 (the "Penal Code"). Violations are punishable by fines or imprisonment for a term not exceeding two years.

Denial-of-service attacks

Seriously hindering, without authorisation, by transferring, harming, deleting, deteriorating, altering or inputting information, without authorisation, and which seriously may disrupt or hinder the operation of a data system, is considered a criminal offence under Section 206 of the Penal Code. Denial-of-service attacks and distributed denial-of-service attacks will typically fall within the scope of Section 206 of the Penal Code. Violations are punishable by fines or imprisonment for a term not exceeding two years.

Phishing

The unauthorised use of another legal person's identity, identity papers, or the unauthorised use of information which may be easily confused with another legal person's identity, with the intent of (i) obtaining an unauthorised benefit for oneself or for another person, or (ii) inflicting a loss on another person, is regarded as an criminal offence under Section 202 of the Penal Code. Accordingly, this provision makes phishing a criminal offence. Violations of Section 202 of the Penal Code are punishable by fines or imprisonment for a term not exceeding two years.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

The infection of IT systems with malware may constitute a criminal offence under several provisions of the Penal Code. Firstly, the possession of malware will as a rule be regarded as a criminal offence under Section 201 of the Penal Code. Section 201 of the Penal Code is further described below. Furthermore, the infection of IT systems with malware which may seriously disrupt or hinder the operation of a IT system, is – as further described above – regarded as a criminal offence under Section 206 of the Penal Code.

Lastly, any person who without authorisation changes, supplements, destroys, deletes or hides another person's data shall be guilty of vandalism under Section 351 of the Penal Code. Accordingly, the infection of IT systems with malware may be regarded as a criminal offence under Section 351 of the Penal Code. Violations of this provision are punishable with fines or imprisonment for a term not exceeding one year. Grand vandalism is punishable with imprisonment for a term not exceeding six years.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

The unauthorised production, procurement, sale, use or distribution of (i) a computer password or other data which may give access to a data system or databased information, or (ii) a computer program or device which is suitable for the purpose of committing a criminal offence, with the intent that it be used for the purpose of committing a criminal offence, is punishable by fines or imprisonment for a term not exceeding one year under Section 201 of the Penal Code. Furthermore, the unauthorised procurement or production of self-spreading data software is also punishable by fines or imprisonment for a term not exceeding one year under Section 201 of the Penal Code. Accordingly, the possession or use of hardware, software or other tools used to commit cybercrime (such as hacking tools) will in certain situations constitute a criminal offence in Norway.

Identity theft or identity fraud (e.g. in connection with access devices)

As mentioned above, the unauthorised use of another legal person's identity, identity papers, or the unauthorised use of information which may be easily confused with another legal person's identity, with the intent of (i) obtaining an unauthorised benefit for oneself or for another person, or (ii) inflicting a loss on another person, is regarded as an criminal offence under Section 202 of the Penal Code. Accordingly, identity theft or identity fraud is regarded as a criminal offence in Norway.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

There are no specific cybercrime provisions under Norwegian law which penalises electronic theft. The general prohibition against theft under Section 321 of the Penal Code only applies to theft of tangible property, and therefore does not apply to electronic theft. Electronic theft can, however, be penalised as forced entry into data systems and access to data systems by unauthorised means (but not the theft as such) under Section 204 of the Penal Code. Violations are punishable by fines or imprisonment for a term not exceeding two years.

Furthermore, both Section 207 and Section 208 of the Penal Code will to a certain extent criminalise electronic theft. Pursuant to Section 207 of the Penal Code, any person who has obtained

knowledge or possession of a trade secret in the course of an assignment, honorary post, employment or business relationship, and which, without authorisation (i) uses the trade secret, or (ii) discloses the trade secret to another person, with the intent of enabling that person to make use of the trade secret, shall be punished with fines or imprisonment for a term not exceeding two years. The foregoing also applies to any person who in the course of an assignment, honorary post, employment or business relationship has been entrusted with technical specifications, descriptions, recipes, models or similar technical materials, and which unlawfully uses the aforementioned documentation during the course of his or her trade.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Violations of the right to private communication is regarded as a criminal offence under Section 205 of the Penal Code, and punishable with fines or imprisonment for a term not exceeding two years. Section 205 of the Penal Code, *inter alia*, applies to the unauthorised:

(i) through use of technical solutions, monitoring and wiretapping of telephone conversations or other communication between other persons, or negotiations held in private meetings which the offender did not participate in, or which the offender obtained without authorisation;

(ii) breaking of a protective measure and other access by unauthorised means to information which is transferred electronically or with technical equipment;

(iii) opening of a letter or other sealed written communication (e.g. encrypted emails or documents) which is addressed to a person other than the offender, or other unauthorised access to such communication; or

(iv) hindering or delaying an addressee from receiving communication by hiding, changing, destroying or delaying the communication.

Failure by an organisation to implement cybersecurity measures

The failure by an organisation to implement cybersecurity measures does not constitute a criminal offence under the Penal Code.

We have, however, described and defined certain sector-specific Applicable Laws in question 2.1, which requires organisations to implement cybersecurity measures. The following Applicable Laws described in question 2.1 envisage criminal sanctions for failure to implement cybersecurity measures:

(a) **The Security Act** Section 31 penalises the failure to implement the cybersecurity measures described in question 2.1 (b) below, with fines or imprisonment for a term not exceeding six months.

(b) **The Financial Supervision Act of 7 December 1956** Section 10 penalises the failure to implement the cybersecurity measures described in question 2.1 (c) below, with fines or imprisonment for a term not exceeding one year.

(c) **The E-com Act** Section 12-4 penalises the failure to implement the cybersecurity measures described in question 2.1 (d) below, with fines or imprisonment for a term not exceeding six months.

(d) **The Energy Act** Section 10-5 penalises the failure to implement cybersecurity measures required under the Emergency Regulation (as further described in question 2.1 (e) below), with fines or imprisonment for a term not exceeding one year.

However, the above-mentioned sanctions may only be imposed if the failure to implement the cybersecurity measure has been intentional or has been caused by gross negligence.

Lastly, we note for the sake of completeness that a failure by an organisation to implement cybersecurity measures under the GDPR and the Personal Data Act (as described in question 1.2A) may not be penalised, and will therefore not constitute a criminal offence.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The Penal Code, albeit with several exceptions, mainly applies to activities carried out in Norway and in Norwegian jurisdictions. However, if the criminality of an act depends on or is influenced by any actual or intended effect, the act shall, pursuant to Section 7 of the Penal Code, also be regarded as committed where the effect has occurred or is intended to be produced. Accordingly, Section 202 and Sections 204–208 may have extraterritorial application if the effect of the relevant offences occurred or was intended to occur in Norway, even if the criminal activity was initiated outside of Norway.

Section 201 of the Penal Code does not for the aforementioned reasons have extraterritorial application, as it only criminalises the unlawful possession and use of certain hacking tools without requiring the occurrence of an effect or the intended occurrence of an effect (e.g. access to an IT system).

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The penalties described in question 1.1 above may be mitigated on the basis of Section 78 of the Penal Code. Mitigating factors of particular relevance in a cybersecurity context under Section 78 of the Penal Code are, *inter alia* (i) that the offender has confessed that he or she has committed the crime, (ii) that the offender has prevented, rectified or limited the damages caused by the offence, or (iii) tried to prevent, rectify or limit the damages caused by the offence.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

The Norwegian Copyright Act of 15 June 2018 (the "**Copyright Act**") includes provisions which prohibit the circumvention of technical protective measures for copyright protected works and computer programs.

Under Section 99 of the Copyright Act, it is prohibited to circumvent effective technical protective measures, designed to prevent or restrict reproduction, communication and/or distribution of copyright protected works to the public. The distribution, production and import for the public and marketing of devices, products or components which:

(i) are promoted, advertised or marketed for the purpose of circumvention;

(ii) have only a limited commercially significant purpose or use other than to circumvent; or

(iii) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention,

of any effective technical protective measure, are also prohibited under Section 99 of the Copyright Act.

Furthermore, Section 101 of the Copyright Act prohibits the sale or possession for commercial purposes of any device for the purpose of circumvention technical protection measures designed to protect computer programs.

Violations of Section 99 and Section 101 of the Copyright Act are punishable with fines or imprisonment for a term not exceeding one year.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

There are currently no general Applicable Laws dedicated to cybersecurity in Norway. Accordingly, the regulatory cybersecurity landscape in Norway is currently fragmented and sector-specific. We have cited certain Applicable Laws of particular relevance below, and indicated which sector/area they apply to:

(a) **The processing of personal data** is subject to:
  (i) the General Data Protection Regulation (Regulation (EU) 2016/679 – the "**GDPR**"); and
  (ii) the Personal Data Act of 15 June 2018.

(b) **The public sector** is subject to:
  (i) the Act relating to Protective Security Services of 20 March 1998 (the "**Security Act**"); and
  (ii) the Regulation on electronic communication with and in the government ("**eGovernment Regulations**").

(c) **The financial services sector** is subject to the Regulation regarding the use of information and communication technology (the "**ICT Regulations**").

(d) **Telecom providers** are subject to:
  (i) the Electronic Communications Act of 4 July 2003 (the "**E-com Act**"); and
  (ii) the Electronic Communications Regulations of 16 February 2004 (the "**E-com Regulations**").

(e) **The energy sector**, i.e. energy providers and entities that are comprised by the nationwide Power Supply Preparedness Organisation (abbreviated as "**KBO**" in Norwegian), are subject to:
  (i) the Act relating to the energy and water resources sector in Norway of 29 June 1990 (the "**Energy Act**"); and
  (ii) the Regulation on Preventive Security and Preparedness in the Energy Supplies of 7 December 2012 ("**Emergency Regulations**").

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

According to the preliminary assessment of the Norwegian Ministry of Justice and Public Security, the Network and Information Systems Directive (the "**NIS Directive**") is relevant for the European Economic Area (the "**EEA**"), and will therefore most likely be transposed into Norwegian law. However, a draft implementation act has not been published and it is currently not clear when the NIS Directive will be effective in Norway.

The current cybersecurity requirements applicable to critical infrastructure in Norway are set out in the Security Act. The Security Act applies to (i) the public sector (i.e., administrative agencies), (ii) certain suppliers of goods or services to administrative agencies, as well as (iii) any other legal person who owns or otherwise controls or supervises sensitive objects (i.e. property which needs to be protected due to national security interests or other vital national interests) or who is granted access to classified information by an administrative agency. Please note that the current Security Act will be replaced by a new Security Act of 1 June 2018, which will become effective during the latter part of 2018.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

As mentioned in question 2.1 above, Norway has a number of Applicable Laws which require organisations to take measures to monitor, detect, prevent or mitigate Incidents. These Applicable Laws and some of the more relevant measures required to be taken under these Applicable Laws are described below:

(a) **Data controllers and processors** are, under the GDPR, required to:
  (i) implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the data processing;
  (ii) notify personal data breaches to the Norwegian Data Protection Authority (the "**NDPA**"); and
  (iii) notify data subjects of any personal data breach, provided that the breach is likely to result in a high risk to the rights and freedoms of natural persons.

(b) **The public sector** is, under the Security Act, required to:
  (i) establish internal control and IT security routines;
  (ii) protect classified information; and
  (iii) notify the relevant supervisory authority if the organisation becomes aware of activities which might pose a threat to security.

(c) **Financial undertakings and similar organisations** are, under the ICT Regulation, required to:
  (i) establish Incident and change management procedures;
  (ii) ensure that the above-mentioned procedures are complied with; and
  (iii) notify the Financial Supervisory Authority of any Incidents that may result in a significant reduction of functionality of the IT systems.

(d) **Telecom providers** are, under the E-com Act and E-com Regulations, required to:
  (a) implement security measures for the protection of communications and data;
  (b) notify subscribers/users and/or authorities of certain security breaches and risks of security breaches; and
  (c) maintain confidentiality about the content of electronic communication and use of electronic communication.

(e) **Energy suppliers** are required to:
  (i) establish routines for protecting and controlling access to sensitive information; and
  (ii) notify and report undesirable Incidents such as data breaches to the authorities.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

The Applicable Laws described in question 2.1 are, to a certain extent, overlapping, and conflict of law issues may arise with respect to

sector-specific legislation. However, there are no specific challenges regarding conflict of law issues within this area.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

As mentioned above, organisations are, under the Applicable Laws described in question 2.1, required to report information related to Incidents to the relevant regulatory/supervisory authorities in Norway. The most generally applicable reporting requirement in Norway related to Incidents is set out in Article 33 of the GDPR, which we have detailed further below:

(a) The reporting obligation under GDPR Article 33 is triggered by a "personal data breach". Pursuant to GDPR Article 4(12), a "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

(b) Personal data breaches are in Norway reported to the Norwegian Data Protection Authority (the "**NDPA**"). So-called "processors" (i.e. organisations which process personal data on behalf of controllers) are required to report the personal data breach to the "controller" (i.e. the organisation which determines the purpose and means of the processing of personal data).

(c) The report must at least:

(i) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and personal data records concerned;

(ii) communicate the name and contact details of the data protection officer or other contact point;

(iii) describe the likely consequences of the personal data breach; and

(iv) describe the measures taken or proposed to be taken by the controller to address the personal data breach.

(d) However, a controller is not obligated to report the personal data breach to the NDPA if it is unlikely that the personal data breach will result in a risk to the rights and freedoms of natural persons.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Organisations may, under Applicable Laws, voluntarily share information related to Incidents or potential Incidents with relevant regulatory/supervisory authorities in Norway. However, the possibility for organisations to share information related to Incidents or potential Incidents to regulatory authorities outside Norway, as well as other private sector organisations, may be limited by statutory confidentiality obligations and similar restrictions.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The following Applicable Laws, described in question 2.1, require organisations to report information related to Incidents to affected individuals:

(a) **GDPR Article 34** requires controllers to inform individuals of personal data breaches that are likely to result in a high risk to the rights and freedoms of the affected individuals (unless the reporting is exempted under GDPR Article 34(3)). The information provided to the affected individual should at least include the information listed in question 2.5 (c), items (ii)–(iv).

(b) **Section 2-7 of the E-com Act** requires telecom providers to notify end users and subscribers of significant risks of security breaches, including security breaches which have (i) damaged or destroyed stored data, or (ii) violated the end user's or subscriber's right to privacy. However, a telecom provider is not obligated to report the aforementioned Incidents to affected individuals if the telecom provider is able to substantiate to the relevant supervisory authority (i.e. the Norwegian Communication Authority) that appropriate security measures have been implemented on the data affected by the Incident. Section 2-7 of the E-com Act does not set out the nature and scope of the information that is required to be reported.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The responses to questions 2.5–2.7 do not change if the notifications include the information provided in items (a)–(e). However, the GDPR may restrict the possibility for organisations to share the information provided in items (b)–(e) above with regulatory authorities outside Norway, as well as private sector organisations in general. The foregoing also applies to any disclosures of price-sensitive information which may be restricted by Norwegian competition legislation.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The following regulators are responsible for enforcing the requirements identified under questions 2.3 to 2.7:

(a) **The Norwegian Data Protection Authority** is responsible for enforcing the requirements set out in the GDPR and the Norwegian privacy legislation.

(b) **The Norwegian National Security Authority** is responsible for enforcing the requirements under the Security Act and the eGovernment Regulations.

(c) **The Norwegian Financial Supervisory Authority** is responsible for enforcing the requirements under the ICT Regulations.

(d) **The Norwegian Communication Authority** is responsible for enforcing the E-com Act and E-com Regulations.

(e) **The Norwegian Water Resources and Energy Directorate** is response for enforcing the requirements under the Energy Act and Emergency Regulations.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The regulators described in question 2.9 are furnished with the following rights with respect to penalties:

(a) **The Norwegian Data Protection Authority** may impose administrative fines of up to EUR 20,000,000, or in the case of an undertaking, 4% of the total worldwide annual turnover. However, infringement of the reporting requirements under the GDPR are limited to EUR 10,000,000, or in the case of an undertaking, 2% of the total worldwide annual turnover.

(b) **The Norwegian National Security Authority** may, *inter alia*, order improvements to IT security and other security measures. Violations of such orders are regarded as a criminal offence under the Security Act, and punishable with fines or imprisonment for a term not exceeding six months.

(c) **The Norwegian Financial Supervisory Authority** may impose coercive fines.

(d) **The Norwegian Communication Authority** may, *inter alia*, impose coercive fines and administrative fines for any infringements of the E-com Act or E-com Regulations.

(e) **The Norwegian Water Resources and Energy Directorate** may impose coercive fines and administrative fines for any infringements of the Emergency Regulations.

Please also see our answer to question 1.1 regarding penalties for failures by an organisation to implement cybersecurity measures, which also applies to this question.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The Personal Data Act, which implemented the GDPR in Norway, was effective on 20 July 2018. The NDPA has, to the best of our knowledge, not imposed any enforcement action for non-compliance with the security and reporting requirements under the GDPR. We are furthermore not aware of any enforcement action taken by the regulators described in question 2.9 in cases of non-compliance with the requirements described in question 2.3 to 2.8.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Please see our answer to question 2.1, which is also applicable to this question.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

As mentioned in relation to question 2.1, above, the financial sector is subject to the ICT Regulations. The telecommunication sector is subject to the E-com Act and the E-com Regulations.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Board members in corporations are liable for damages caused by negligence pursuant to the general compliance principles under Section 6-13 and 17-1 of the Norwegian Limited Liability Companies Act. Members of the board may therefore be held liable for not establishing appropriate security measures and/or otherwise failing to prevent, mitigate, manage or respond to an Incident.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

In summary, the following companies are, under the Applicable Laws described in question 2.1, required to implement the measures in items (a)–(d):

(a) Energy suppliers are, under Section 2-2 of the Emergency Regulations, required to designate a CISO.

(b) Telecom providers, companies in the finance sector, KBOs and the public sector are required to establish a written Incident response plan or policy. Most companies processing personal data are also required to establish such plans under GDPR Article 32.

(c/d) Telecom providers, companies in the finance sector, KBOs, the public sector and most companies processing personal data are required to conduct a cyber risk assessment, including penetration tests and/or vulnerability assessments.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Norwegian companies are not subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents. Listed Norwegian Companies are generally obligated to disclose information which may be of significance to, e.g., value of the shares. The foregoing may in certain situations also obligated the listed company to disclose information in relation to cybersecurity risks and/or Incidents.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Please see our answer to question 2.3, where we have summarised other specific requirements under Applicable Laws in relation to cybersecurity.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In our assessment, the most significant exposure to civil actions in relation to any Incident arises out of the GDPR. Under GDPR Article 82, any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered. Furthermore, a person may under Section 30 of the Personal Data Act also claim damages for non-economic loss as a result of an infringement of the GDPR.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

The following two cases have been brought in Norway in relation to Incidents:

(a) TBERG-2017-164611 (hacking/unauthorised access); and

(b) TNERO-2013-89352 (several denial-of-service attacks).

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Any person who negligently or wilfully causes an Incident may, under the Norwegian law of torts, be held liable for any foreseeable loss which has occurred due to the negligent or wilful act.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Organisations are permitted to take out insurance against Incidents in Norway.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are, to the best of our knowledge, no regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There are no specific requirements under Applicable Law regarding items (a) and (b) above.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

The provisions on whistleblowing set out in the Working Environment Act of 17 June 2005 will in our assessment not limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee. However, the Regulations on employers' access to employees' email accounts, etc. of 2 July 2018 restricts the possibility for employers to access employees' email accounts, personal folders on the company's IT systems, and devices used by the employees. The aforementioned Regulations may therefore potentially restrict Norwegian employers' possibility to identify Incidents or potential Incidents caused by an employee.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcement (i.e. the police and prosecution authorities) may, *inter alia*, rely upon the following investigatory powers under the Criminal Procedure Act of 22 May 1981 (the "**Criminal Procedures Act**"):

(i) to search of a person, location, vehicle and data systems;

(ii) to confiscate evidence;

(iii) to confiscate electronically stored data, including from providers of electronic communication services and networks; and

(iv) to order any person who has dealings with a data system to provide information which is necessary to enable the law enforcement to access the data system (e.g. passwords and encryption keys).

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no requirements under Applicable Laws for organisations to implement backdoors in their IT systems. However, pursuant to Section 199a of the Criminal Procedure Act, law enforcement authorities may, in connection with searches of data systems, order any person who has dealings with the data system to provide information which is necessary to enable the law enforcement authorities to access the data system, or to open it with biometric data.

Christopher Sparre-Enger Clausen
Advokatfirmaet Thommessen AS
Haakon VIIs gate 10
PO box 1484 Vika
NO-0116 Oslo
Norway

Tel: +47 23 11 11 41
Email: csc@thommessen.no
URL: www.thommessen.no

Partner Christopher Sparre-Enger Clausen is the Head of Thommessen's Technology and Data Protection Group and has over 12 years of experience within the practice area.

His experience includes a broad range of practice areas, such as software licensing, cloud services, big data projects, technology development contracts, outsourcing projects, regulatory compliance, IPR and dispute resolution on large IT projects. He is also regularly engaged in M&A work involving technology and telecom businesses in Norway and internationally. He increasingly assists a wide range of clients on privacy (GDPR)-related projects and regulatory compliance.

Christopher has achieved a high degree of industry sector expertise within technology-related industries, specifically within IT and digital transformation.

Uros Tosinovic
Advokatfirmaet Thommessen AS
Haakon VIIs gate 10
PO box 1484 Vika
NO-0116 Oslo
Norway

Tel: +47 23 11 14 44
Email: uto@thommessen.no
URL: www.thommessen.no

Uros is an associate in Thommessen's Technology and Data Protection Group. He works in matters concerning IT and data protection as well as intellectual property. Uros is frequently engaged in large IT projects and complex data protection matters (including, e.g., cross-border data transfer arrangement, risk assessments and data processing agreements). Uros also has considerable experience with matters pertaining to cybersecurity, copyright, including use of open-source licensed material. Uros holds a Master's degree from the University of Oslo, having written a Master's thesis on the legal protection of technological protection measures.

THOMMESSEN

Established in 1856, Thommessen is considered to be one of Norway's leading commercial law firms. The firm has offices in Oslo, Bergen, Stavanger and London. The firm provides advice to Norwegian and international companies as well as organisations in the public and private sectors, ranging from SMEs to large multi-national corporations. Thommessen covers all business related fields of law. 180 lawyers work at Thommessen today.

As the world has undergone a technological revolution, our lawyers have very much been a part of the development of the industry along the way. We have assisted our clients and helped develop the framework necessary to adjust to new technological advances. Thommessen assists leading Norwegian and international companies, both on the customer and supplier side, in cases involving everything from IT procurement to development projects and licensing of technology and data security.

Philippines

Leland R. Villadolid Jr.

Angara Abello Concepcion Regala & Cruz Law Offices

Arianne T. Ferrer

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes, hacking is a criminal offence under Republic Act No. 8792 or the Electronic Commerce Act ("ECA"). Hacking is defined as (1) unauthorised access of or interference with computer systems, servers, or other information and communication systems, (2) unauthorised access to corrupt, alter, steal, or destroy electronic data using computers or other information and communication systems without the computer or system owner's knowledge and consent, or (3) the introduction of computer viruses resulting in the corruption, alteration, theft, or loss of such data.

Hacking is punished by a maximum fine in an amount commensurate to the damage incurred. A mandatory penalty of imprisonment between six months and three years shall be meted out in either case.

Hacking, when it involves illegal access or interception, data interference, or system interference that affects the confidentiality, integrity, and availability of electronic data or computer systems, is also punished as a criminal offence under Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 ("CPA") by a maximum fine in an amount commensurate to the damage incurred. An additional penalty of imprisonment of six years and one day to 12 years (*prision mayor*) may also be imposed.

Criminal cases are pending prosecution before the courts.

Denial-of-service attacks

Yes, a denial-of-service attack ("DOS attack") is a criminal offence under the CPA because it involves system interference that affects the availability of electronic data or computer systems.

Criminal cases are pending prosecution before the courts.

Phishing

Yes, phishing is penalised under the CPA as an offence relating to computer-related forgery, fraud and/or identity theft. An attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication ("phishing"), is punishable by a maximum fine of PHP 200,000.00 and/or imprisonment of *prision mayor*.

Criminal cases are pending prosecution before the courts.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes, the infection of IT systems with malware is a criminal offence. It may be punished as hacking under the ECA or as an offence against the confidentiality, integrity and availability of computer data and systems under the CPA.

Under the ECA, the infection of IT systems with malware is punishable by a maximum fine in an amount commensurate to the damage incurred and imprisonment for a period of between six months and three years. Under the CPA, the same act is punishable by a maximum fine in an amount commensurate to the damage incurred and/or imprisonment of *prision mayor*. If the act is committed against critical infrastructure of the Philippines, the penalty is a maximum fine in an amount commensurate to the damage incurred and/or imprisonment for a period of between 12 years and 20 years and one day (*reclusion temporal*).

Criminal cases are pending prosecution before the courts.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Yes, the possession of cybercrime tools is a criminal offence. The possession of a device (including a computer program) that may be used to perpetrate any offence under the CPA, when coupled with the intent to use such device unlawfully, is punishable by a maximum fine of PHP 500,000.00 and/or imprisonment of *prision mayor*.

Criminal cases are pending prosecution before the courts.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity theft, when defined as the intentional acquisition, use, transfer, possession, alteration, or deletion of identifying information belonging to another natural or juridical person without right, is a criminal offence under the CPA. Identity theft is punishable by a maximum fine in an amount commensurate to the damage incurred and/or imprisonment of *prision mayor*.

The unauthorised or fraudulent use of an access device (any card, plate, code, account number, electronic serial number, personal identification number, telecommunications service, equipment or instrument, or other means of account access that may be used to obtain anything of value or to initiate a fund transfer) belonging to another natural person is prohibited under Republic Act No. 8484 or the Access Devices Regulation Act of 1998 ("ADRA"). It is punishable by a maximum fine of PHP 10,000.00 or twice the value obtained (whichever is greater) and imprisonment for a period of between six years and 10 years. If the perpetrator was previously convicted of another offence under the ADRA, the punishment is a maximum fine and/or imprisonment for a period of between 12

years and 20 years. Notably, "identity theft" or "identity fraud" is not expressly defined under the ADRA.

Criminal cases are pending prosecution before the courts.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Criminal copyright infringement is covered by Sections 177, 193, 203, 208 and 211 in relation to Section 217 of the Intellectual Property Code. The penalty for infringement of electronic data or through electronic means is one degree higher than imprisonment for a period of between one year and three years and a fine between PHP 50,000.00 and PHP 150,000.00.

Though a case that deals squarely with criminal copyright infringement of electronic data has yet to reach the Supreme Court, criminal copyright infringement was discussed in the context of a news video in *ABS-CBN Corporation v. Gozun*. In that case, the Supreme Court held that audio-visual work, like a news video, is protected from the moment of its creation, regardless of its "mode or form of expression". Accordingly, the unauthorised reproduction, distribution, or communication of audio-visual work through electronic means would be punishable as criminal copyright infringement.

One should note that Section 30 of the ECA limits a service provider's liability for criminal copyright infringement to instances when the service provider (1) had actual knowledge of the unlawful act, (2) received financial benefit from the unlawful act, and (3) did not directly commit or cause another person to commit the unlawful act. Unlawful acts include any activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

Offences against the confidentiality, integrity, and availability of electronic data and computer systems, e.g., illegal access, illegal interception, data interference, system interference, misuse of devices, and cyber-squatting, are punishable under the CPA. Except for misuse of devices, these offences are punishable by a maximum fine in an amount commensurate to the damage incurred or imprisonment of *prision mayor*. For an offence involving misuse of devices, the penalty is a maximum fine of PHP 500,000.00 and/or imprisonment of *prision mayor*.

Further, when these offences are committed by a natural person on behalf of a juridical person (provided that the natural person was authorised and acted within the scope of such authority), the juridical person shall be given a maximum fine of PHP 10,000,000.00.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The Philippine National Police Anti-Cybercrime Group ("PNP-ACG") regularly releases cybersecurity updates through issuances of security bulletins on its website, designed to raise public awareness of potential threats, vulnerabilities in their systems and information on better protection of their IT environment. Aside from these security bulletins, the PNP-ACG also updates its database to inform, educate and protect the public on cybercrime issues, internet frauds and scams and gives suggestions on how to address them.

Failure by an organisation to implement cybersecurity measures

Yes, a juridical person's failure to take appropriate measures to protect its computer systems, servers, or information and communication systems may be a criminal offence.

Under Republic Act No. 10173 or the Data Privacy Act of 2012 ("DPA"), a juridical person, who allowed a crime involving personal data to occur through fault or negligence, shall have its rights as a data subject suspended or revoked. The DPA's implementing rules and regulations state that failure to implement security measures for the protection of personal data may lead to civil and criminal liability.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Section 21 of the CPA gives Regional Trial Courts ("RTC") in the Philippines jurisdiction over cybercrimes committed by Filipino citizens, regardless of the place of commission.

Section 6 of the DPA provides for extraterritorial application over acts committed by Filipino citizens or entities with a link to the Philippines, e.g., entities that do business in the Philippines, collect or store personal information in the Philippines, or enter into contracts in the Philippines, as well as acts committed against Filipino citizens or residents.

For other laws defining and punishing offences involving cybersecurity that do not expressly provide for extraterritorial application, Article 14 of the Civil Code applies (penal laws only cover acts or omissions committed within Philippine territory, subject to customary or conventional international law).

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Applicable Laws do not provide actions that mitigate or absolve a perpetrator from criminal liability arising from cybersecurity offences. However, for offences punishable under the Revised Penal Code ("RPC") and committed with a cybercrime element, the rules on mitigating, justifying, and exempting circumstances found in Articles 11 through to 13 of the RPC apply.

Notably, notification is itself an obligation under the DPA, such that failure to notify the proper authority of an Incident may amount to a violation of the DPA.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

All crimes defined and punished under the RPC and special penal laws, when committed through information and communication systems and technology, shall be covered by the CPA. The general effect is that the penalties shall be increased one degree higher than the imposable penalties under the RPC and special penal laws.

Incidents can be considered terrorism when (1) they are performed to accomplish the following: piracy or mutiny; rebellion or insurrection; *coup d'état*; murder; kidnapping and serious illegal detention; and other crimes of destruction enumerated in Section 3 of Republic Act No. 9372 or the Human Security Act of 2007 ("HSA"), and (2) they cause widespread and extraordinary fear and panic among the public in order to coerce the government to give in to an unlawful demand.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The ECA, ADR, DPA, CPA, Republic Act No. 10844 or the Creation of the Department of Information and Communications Technology Act ("DICTA"), Republic Act No. 10627 or the Anti-Bullying Act ("ABA"), Republic Act No. 8293 as amended by Republic Act No. 10372 or the Intellectual Property Code ("IPC"), and their respective implementing rules and regulations.

Other laws, orders, rules, and regulations related to cybersecurity are: Supreme Court Administrative Matter No. 01-7-01-SC or the Rules on Electronic Evidence; Republic Act No. 10867 or the National Bureau of Investigation Reorganization and Modernization Act; Executive Order No. 189 or the Creation of the National Cyber-Security Inter-Agency Committee; and the HSA with respect to Sections 3 and 7.

On 19 February 2018, the Senate unanimously concurred on the ratification of the Budapest Convention on Cybercrime. The Budapest Convention seeks to pursue a common criminal policy aimed to protect society against cybercrime, harmonise procedural laws, improve investigative techniques and gathering of electronic evidence, and foster multilateral cooperation. The Philippines' accession to the Convention signifies the government's acknowledgment of cybercrime not only in a domestic setting but on an international level, and shows the country's resolve in addressing cybercrime as a major threat to national security.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

There is as yet no specific law enacted. However, the Department of Information and Communications Technology ("DICT") launched a national cybersecurity strategy framework that will ensure the protection of critical infrastructure from cyber attacks through effective coordination with law enforcement agencies. National Cybersecurity Plan 2022, which seeks to safeguard the ICT environment of the country through the establishment of a robust cybersecurity infrastructure, is intended to ensure the continuous operation of the country's critical infrastructure, public and military networks, to implement cyber-resiliency measures to enhance the ability to respond to threats before, during and after cyber attacks, and to implement a public awareness campaign on cybersecurity measures.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the DPA, a juridical person must take reasonable and appropriate organisational, physical and technical measures to protect personal information from unlawful destruction, alteration, disclosure, access, and other unlawful processing. These measures must include: (1) safeguards to protect the juridical person's computer network against use of or interference with the network's functionality or availability; (2) a security policy for processing personal information; (3) a process for identifying and accessing reasonably foreseeable vulnerabilities in the network and for taking preventive and corrective action against Incidents; (4) regular monitoring of Incidents; (5) the juridical person's personal information controller must ensure that third parties processing personal information on the juridical person's behalf will similarly take reasonable and appropriate measures; and (6) the juridical person's personal information controller must promptly notify the National Privacy Commission ("NPC") and affected data subjects when an Incident resulted in a security breach.

The DPA's implementing rules and regulations provide guidelines on measures to be taken by a juridical person dealing with personal information. They highlight the key principles for the protection of personal data: availability; integrity; and confidentiality.

The suggested organisational security measures are: (1) employing compliance officers or protection officers; (2) creating and implementing policies that take into account the nature, scope, context and purposes of the information processing, as well as the risks posed to the rights and freedoms of data subjects; (3) maintaining records that sufficiently describe the data processing system and identifying the duties and responsibilities of employees who have access to personal data; (4) ensuring that employees keep information confidential even after leaving their positions; (5) developing, implementing, and reviewing the procedure for personal data collection, access management, system monitoring, and protocols to be taken after Incidents occur as well as policies for the exercise of rights by data subjects, the retention of personal data, and the processing of information only for declared, specified, and legitimate purposes; and (6) ensuring that personal information processors take measures in accordance with the DPA.

The suggested physical security measures are: (1) implementing policies and procedures to monitor and limit access to facilities where electronic data can be used; (2) designing facilities to ensure privacy of personal information processors; (3) clearly defining duties, responsibilities, and schedules of personal information processors such that only those performing their official duties have access to electronic data at a given time; and (4) implementing policies and procedures to prevent mechanical destruction of files and equipment and to protect against natural disasters, power disturbances, external access, and other reasonably expected threats.

The suggested technical security measures are: (1) ensuring the ability to restore availability and access to personal data in a timely manner in the event of an Incident; (2) testing, assessing, and evaluating the effectiveness of security measures regularly; (3) encrypting personal data for storage and while in transit; and (4) implementing authentication processes and other technical security measures that control and limit access to information.

In determining whether a juridical person has taken reasonable and appropriate security measures, the NPC shall consider the nature of the personal data that requires protection, the risks posed by the processing, the size of the organisation and complexity of its operations, current data privacy best practices, and the cost of security implementation.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

The Supreme Court has yet to hear and resolve any conflict-of-laws specifically in relation to cybersecurity. The DPA does not cover personal information that was collected in a foreign jurisdiction in a manner that complies with Applicable Laws of that jurisdiction. However, security measures must still be undertaken when there is processing of personal information, regardless of the place of collection.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

A personal data breach is defined as a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed". A personal data breach exists when (1) sensitive personal information that may be used to commit identity fraud is reasonably believed to have been acquired by an unauthorised person, and (2) the personal information controller believes that such acquisition poses a real risk of harm to the affected data subjects.

Under the DPA, the personal information controller must inform the NPC and affected data subjects within 72 hours of the former's knowledge or reasonable belief that a personal data breach has occurred.

On one hand, the notification to the affected data subjects should contain the nature of the breach, the personal data possibly involved, and the measures taken by the entity to address the breach. It should also contain measures taken to reduce the harm or negative consequences of the breach, the contact details of representatives of the personal information controller so that data subjects can obtain additional information about the breach, and the assistance to be provided. On the other hand, the notification to the NPC should include the nature of the breach and the measures taken to remedy the breach but exclude any description of the personal privileged information.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

A juridical person processing personal information is not absolutely prohibited from sharing non-personal information related to Incidents by the DPA. On the other hand, personal information may be shared but with the consent of the affected data subject.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

A juridical person processing personal information is required to notify the affected data subjects in case of a personal data breach, in the same manner as discussed in question 2.5. The notification to the affected data subjects shall also contain instructions on how they may acquire more information on the breach.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, once there has been a personal data breach, a juridical person, through its personal information controller, must notify the affected data subjects. The personal privileged information itself shall not be disclosed to any party, including the NPC, without the consent of the affected data subjects.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The regulator tasked to ensure compliance with the DPA is the NPC, which is an independent body mandated to administer and implement the DPA and to monitor and ensure the Philippines' compliance with international personal data protection standards. The NPC is attached to the DICT, though it performs its functions independently.

The NPC is a collegial body composed of one commissioner and two deputy commissioners. Its functions are: rule-making; advising; educating; compliance and monitoring; adjudicating complaints and investigations; and enforcing the DPA. Further, the NPC may issue official directives and administrative issuances, orders, and circulars that deal with procedural rules, schedules of administrative fines and penalties, and procedures for registration of data processing systems and notification.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The DPA does not expressly penalise the failure to adopt the suggested reasonable and appropriate measures or to submit the required notification, except with respect to persons found to have intentionally concealed the existence of a personal data breach despite knowing of the breach and the obligation to notify the NPC. In such case, concealment shall be punishable by imprisonment for a period of between one year and six months and five years as well as a fine of not less than PHP 500,000.00, but not more than PHP 1,000,000.00.

Additionally, persons who allow unauthorised access to personal data shall be punished by imprisonment ranging from one year to

three years and a fine of not less than PHP 500,000.00, but not more than PHP 2,000,000.00. Persons who allow unauthorised access to sensitive personal information shall be punished by imprisonment ranging from three years to six years and a fine of not less than PHP 500,000.00, but not more than PHP 4,000,000.00.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In January 2018, the NPC directed Globe Telecom, Inc., a leading provider of telecom services, to enforce more stringent subscriber verification protocols when one of its prepaid mobile customers fell victim to identity theft, which was perpetrated through unauthorised access to the customer's online banking account. This "SIM swap scheme" involves a perpetrator illegally obtaining a replacement SIM card from a telecom operator belonging to another and using the number for fraudulent activities. The *modus* involves the perpetrator posing as the owner of the number and claiming the original SIM card is stolen. In getting access to the mobile number, the perpetrator is able to access the owner's online banking and other personal accounts and use it in various transactions by exploiting the one-time password mobile authentication functions of the owner's registered mobile number.

Following this Incident, NPC directed Globe Telecom, Inc. to upgrade the latter's security procedures and tasked the telecom company to look into security gaps in its SIM replacement procedures. As a result, the latter committed to enforce a 24-hour delay in the activation of newly replaced SIM cards to subscribers who report either a lost or stolen phone, if the subscriber cannot present the original SIM bed or provide government-issued ID cards as proof of identification.

In March 2018, following the controversy wherein Aleksandr Kogan's personality quiz was installed by Facebook users and personal data was improperly shared with Cambridge Analytica, the NPC opened an investigation on Facebook to establish the scope and impact of the Incident on Filipino users and possible violations of the DPA. Notably, it was found that the Philippines was the second-most affected country in terms of data subjects. As a result, Facebook gave its plans to restrict data access of third parties on Facebook starting 9 April 2018, and in the process, users shall be notified if there was unauthorised processing of their personal data by Cambridge Analytica.

The NPC may compel government entities, agencies and instrumentalities to take specific actions to comply with the DPA. More generally, pursuant to its investigation of a complaint, adjudication of a dispute, or preparation of a report, the NPC may also issue cease-and-desist orders and impose a temporary or permanent ban on the processing of personal information.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Applicable Laws on cybersecurity generally do not differ across different industries. However, under the DPA, the requirement to register processing operations and to notify the NPC of any changes to the automation of such processing operations only applies to a juridical person with 250 or more employees or with more than a *de minimis* amount of data subjects with sensitive personal information (at least 1,000 data subjects).

Meanwhile, under the ADRA, companies engaged in the business of issuing access devices (usually banks, financing companies, and other financial institutions) are required to report any fraudulent acts involving access devices that were committed in the previous calendar year to the Credit Card Association of the Philippines.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The Bangko Sentral ng Pilipinas ("BSP") is the primary regulator of the financial services sector. The BSP issued BSP Circular No. 808 series of 2013 which provides guidelines on Information Technology Risk Management for all banks and BSP-supervised financial institutions ("BFSP"). The BSP is currently in the process of drafting a circular that would introduce amendments to Circular 808: incorporating the latest standards on information security; and presenting a more holistic information technology security management system integrated with the information security programs and risk management systems of banks. Other pertinent issuances of the BSP are: Circular No. 859 series of 2014, which requires banks and BFSPs to migrate from magnetic stripe technology to chip-enabled technology based on Europay, MasterCard and Visa ("EMV"); Circular No. 863 series of 2016, which are guidelines on the implementation of EMV Card Fraud Liability Shift Framework (banks and BFSPs that have not yet shifted to EMV technology shall be allowed subject to the condition that they will be held responsible for losses associated with the use of counterfeit cards in a card-present environment); and Circular No. 958 series of 2017, which are guidelines for banks and BFSPs in implementing multi-factor authentication as a replacement for single-factor authentication in their systems.

The DICT and the National Telecommunications Commission, which regulates the telecommunications sector, have yet to issue specific legal requirements relating to cybersecurity. However, the DICT recently launched a national cybersecurity strategy framework that will ensure the protection of critical infrastructure from cyber attacks through effective coordination with law enforcement agencies (National Cybersecurity Plan 2022).

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Under the CPA, if the commission of a punishable offence was made possible by the lack of supervision or control by a natural person with a leading position who acts individually or on behalf of a juridical person and said natural person has a power of representation or is otherwise authorised to make decisions and act on behalf of the juridical person, the juridical person shall be fined an amount of double the imposable fines under Section 7 or PHP 5,000,000.00 (whichever is higher).

Under the DPA, if a juridical person has committed a punishable offence, the responsible officers who participated in or allowed, through gross negligence, the offence to be committed may be prosecuted.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Under the DPA, a Data Privacy Officer ("DPO") must be registered with the NPC if a company has more than 250 employees or the processing of personal information is: (1) likely to pose a risk to data subjects' rights and freedoms; (2) not occasional; or (3) involves sensitive personal information of at least 1,000 individuals. The application for registration shall include the name and address of the personal information controller or processor, the general description of privacy and security measures for data protection and copies of all policies relating to data governance, data privacy and information security.

Thus, the DPA does not specifically require the designation of a Chief Information Security Officer ("CISO"), only the designation of a DPO. However, with respect to (b), (c) and (d), while not specifically stated in the DPA, they may be deemed reasonable requirements to implement the objectives of the DPA.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Under the DPA, the NPC requires the annual submission of a summary of documented security Incidents and personal data breaches.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Yes. When ordered by a court to preserve or examine computer data, service providers (public or private entities that provide a service that allows users to communicate by means of a computer system, or any other entity that processes or stores computer data on behalf of users) are required to: (1) preserve the integrity of traffic data and subscriber information for a minimum period of six months from the date of the transaction; (2) preserve the integrity of content data for six months from the date of receipt of the order from law enforcement or competent authorities requiring its preservation; (3) preserve the integrity of computer data for an extended period of six months from the date of receipt of the order from law enforcement or competent authorities requiring extension on its preservation; (4) preserve the integrity of computer data until the final termination of the case and/or as ordered by the court, as the case may be; (5) ensure the confidentiality of the preservation order and its compliance; (6) collect or record by technical or electronic means and/or cooperate and assist law enforcement or competent authorities in the collection or recording of computer data covered by the court warrant; (7) disclose or submit users' information, traffic or relevant data to law enforcement or competent authorities within 72 hours from receipt of the court warrant; and (8) immediately and completely destroy the computer data that is the subject of a preservation order after the expiration of the period provided under the CPA.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Civil actions involving Incidents may be brought before the proper court in two cases: (1) an action to demand the civil liability arising from a criminal offence under Article 30 of the Civil Code; and (2) an action to demand indemnification for damage to human relations under Articles 19 through to 21, 26 and 32 of the Civil Code.

Articles 19 through to 21 of the Civil Code are catch-all provisions to hold a person civilly liable for his injurious act or omission. Article 19 requires a person to act with justice, give everyone his due, and observe honesty and good faith. If a person wilfully or negligently causes damage to another person contrary to Article 19, he must indemnify the latter pursuant to Article 20. Similarly, a person who causes damage to another person contrary to morals, good customs, or public policy shall compensate the latter under Article 21.

Article 26 of the Civil Code requires a person to respect the dignity, personality, privacy and peace of mind of another person. Violating another person's privacy in relation to his residence under this provision and to his communication and correspondence under Article 32 of the Civil Code allows the offended party to recover damages.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

The Supreme Court has yet to resolve a case involving civil and criminal actions arising from Incidents. It did, however, rule on the CPA's constitutionality in *Disini v. Secretary of Justice*. Before the lower courts, most cases with a cybersecurity element are criminal actions for computer hacking, child pornography, cybersex, ATM fraud and libel.

In 2016, the NPC issued a decision in NPC Case No. 16-001, which ruled that the COMELEC violated the DPA after the group Anonymous hacked the Philippines' voter registration database. The hack involved at least 75,302,683 voter records and 1,267 COMELEC employee records. The NPC found that the COMELEC Chairman wilfully and intentionally disregarded his duties as a personal information controller and recommended his prosecution under the CPA.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes. Incidents may lead to liability based on quasi-delict. Under Article 2176 of the Civil Code, a person whose act or omission injures another person, whether through fault or negligence, is liable to pay damages to the latter.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, with prior approval, the Insurance Commission ("IC") allows cyber-insurance products in the Philippines. Cyber-insurance may offer protection against losses due to: improper denial or approval

of access to data; breach of computer software, system or security; or theft of computer hardware, among others. Cyber-insurance may also include protection against extortion and loss as a result of an Incident and payment for an investigation to determine the source thereof. Thus, cyber-insurance may address loss resulting from cyber attacks, e.g., "Wannacry" ransomware.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Generally, there are no regulatory limitations to insurance coverage against the types of losses mentioned above. However, exceptionally, the insured cannot recover amounts paid arising from damages, fines or penalties that are exemplary in nature. Likewise, there is no recovery for amounts paid arising from the insured's wilful and/or intentional violation of the DPA.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

Under the DPA, covered juridical persons must have systems and processes in place to make their employees aware of their responsibilities (ensuring integrity, availability and confidentiality of data) and the organisational requirements that must be met to comply with the DPA.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

Yes, Applicable Laws did not amend or repeal the Secrecy of Bank Deposits Act (Republic Act No. 1405), the Foreign Currency Deposits Act (Republic Act No. 6426), the Credit Information System Act (Republic Act No. 9510), and the Anti-Money Laundering Act (Republic Act No. 9610). Thus, these acts may prevent the reporting of Incidents to the proper authorities.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Under Section 7 of the HSA, law enforcement authorities may listen to, intercept and record, with the use of any mode, form, kind or type of electronic or other surveillance equipment or intercepting and tracking devices, or with the use of any other suitable ways and means for that purpose, any communication, message, conversation, discussion, or spoken or written words between members of a judicially declared and outlawed terrorist organisation, association, or group of persons or of any person charged with or suspected of the crime of terrorism or conspiracy to commit terrorism, upon written order of the Court of Appeals. However, Section 7 is limited by Section 44 of the DPA, which requires law enforcement authorities to comply with the principles of transparency, proportionality, and legitimate purpose.

Under the CPA, the National Bureau of Investigation ("NBI") and the PNP Cybercrime Unit are responsible for enforcement. They are authorised to collect traffic data in real time, with due cause as evidenced by a court warrant. They may also issue an order requiring any person or service provider to disclose relevant information or data in his possession and control within 72 hours from receipt, also after securing a court warrant.

The NBI and the PNP may perform the following, upon securing a search and seizure warrant and within the time period provided therein: (1) secure a computer system or a computer data storage medium; (2) make and retain a copy of computer data secured; (3) maintain the integrity of the relevant stored computer data; (4) conduct forensic analysis or examination of the computer data storage medium; and (5) render inaccessible or remove computer data in the accessed computer or network. Further, they may order any person, who has knowledge of the computer system, server, or information and communication system and the measures to protect and preserve the electronic data therein, to assist in the search and seizure.

When computer data is found to *prima facie* violate the CPA, the Department of Justice may issue an order to restrict or block access to the data.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, juridical persons are not required to leave backdoors in their information and communication systems or to give law enforcement officers encryption keys.

Acknowledgment

The authors would like to thank Aileen P. Cruz, Associate of the Litigation & Dispute Resolution Department, for her invaluable assistance in the preparation of this chapter.

Tel: +632 830 8329 / Email: apcruz@accralaw.com

Leland R. Villadolid Jr.
Angara Abello Concepcion Regala & Cruz Law Offices
ACCRALAW Tower
Second Avenue Corner 30th Street
Crescent Park West
Bonifacio Global City, 1635 Taguig, NCR
Philippines

Tel: +632 830 8131
Email: lrvilladolid@accralaw.com
URL: www.accralaw.com

Mr. Villadolid is a Senior Partner of the Litigation & Dispute Resolution Department. He obtained his Bachelor of Laws from the Ateneo de Manila University. He also holds a Bachelor of Arts in Philosophy from the University of the Philippines. His postgraduate education includes a Master of Laws from the George Washington University and training at the Environmental Law Institute in Washington, D.C.

Mr. Villadolid is a consultant of the following: Information Security Officers Group (ISOG); and the Philippine National Police Anti-Cybercrime Group (PNP-ACG) Advisory Council. He is also a member of the Philippine Dispute Resolution Center, Inc. (PDRCI) and Forum for International Irregular Network Access (FIINA). Finally, Mr. Villadolid serves as a Commissioner in the Commission on Bar Discipline of the Integrated Bar of the Philippines (IBP).

Mr. Villadolid handles cases involving litigation and/or arbitration on information communication and technology, cybercrimes, public utilities, antitrust and trade regulation and white-collar crimes.

Arianne T. Ferrer
Angara Abello Concepcion Regala & Cruz Law Offices
ACCRALAW Tower
Second Avenue Corner 30th Street
Crescent Park West
Bonifacio Global City, 1635 Taguig, NCR
Philippines

Tel: +632 830 8329
Email: atferrer@accralaw.com
URL: www.accralaw.com

Ms. Ferrer is an Associate of the Litigation & Dispute Resolution Department. She obtained a *Juris Doctor* degree from the University of the Philippines College of Law in 2015 and a Bachelor of Science degree in Business Economics from the University of the Philippines, where she graduated *cum laude* in 2010. While at law school, Ms. Ferrer served as an editor of the *Philippine Law Journal* and represented the Philippines in the Philip C. Jessup International Law Moot Court Competition.

Ms. Ferrer was admitted to the Philippine Bar in 2016. Since then, she has handled litigation, alternative dispute resolution, and arbitration cases involving civil and commercial disputes. Ms. Ferrer has acted as an administrative secretary in arbitration proceedings before the International Commercial Court and the Philippine Construction Industry Arbitration Commission.

ACCRALAW®

ANGARA ABELLO CONCEPCION REGALA & CRUZ ("ACCRALAW") is a multi-disciplinary team of legal professionals with in-depth knowledge in specialised fields of law. Seven practice departments in three regions offer timely, creative, and strategic legal solutions matched with cost-efficient administration and expert handling of client requirements.

ACCRALAW is the undisputed leader in Philippine litigation and alternative dispute resolution ("ADR"). With a deep bench of litigators and ADR practitioners and a consistent, outstanding track record covering more than 40 years, ACCRALAW has extensive expertise in handling large-scale and complex disputes. Its trial experience before courts, tribunals, administrative agencies, and ADR fora is unmatched. ACCRALAW has contributed to Philippine jurisprudence by successfully representing clients in landmark legal controversies.

ACCRALAW's pre-eminence in litigation and ADR is due to the structured, hands-on training of its junior lawyers, who are among the top graduates in the Philippines, and the wide areas of expertise and the varied experience of its senior lawyers. Most ACCRALAW lawyers have completed postgraduate studies abroad, while others are faculty members of the best law schools. ACCRALAW lawyers have been commissioned by the Supreme Court to revise the Rules of Court and draft other rules in connection with the practice of law.

Portugal

Miguel Duarte Santos

Gouveia Pereira, Costa Freitas & Associados, S.P. R.L.

Sofia Gouveia Pereira

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes, under the Cybercrime Law (Law no. 109/2009), access to a system or part of it without authorisation, as well as unauthorised access to sell, distribute or generate a code or computer data that produces unauthorised actions, are offences punishable with one year's imprisonment or a fine.

Denial-of-service attacks

Yes. Under the Cybercrime Law, unauthorised access with the objective to hinder, disrupt, obstruct or interrupt the normal activity of a computer by altering, deleting, damaging software or data and by any other method interfering with a computer, is punishable with a maximum sentence of five years' imprisonment or 600 daily fines.

Phishing

Yes. Under the Cybercrime Law, actions with the intention of deception that interfere in a legal relationship or actions such as the use of false data or obtainment of documents with the intention of having them used for legally relevant purposes are punishable with a maximum sentence of five years' imprisonment or 120 to 600 daily fines. If these actions regard bank card data or any other system or means of payment, a communications system or any system with limited access, the offence is punishable with one to five years' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. Infection of IT systems with malware would be considered computer sabotage under the Cybercrime Law. Any action without authorisation with the objective of hindering or perturbing the normal functioning of IT systems through the introduction, damage, change, deletion or denial of access to software or IT systems is punishable with a maximum sentence of five years' imprisonment or 600 daily fines. The introduction of software with the objective of having computers or other devices acting without the owners' authorisation is punishable with a maximum sentence of three years' imprisonment or a fine.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

The possession, with the intention to produce, sell, distribute or in any other way disseminate, of software or computer data designed to commit the crimes foreseen in the Cybercrime Law is a criminal offence.

Identity theft or identity fraud (e.g. in connection with access devices)

Yes, under the Cybercrime Law, theft or identity fraud could be considered "IT falsehood" (article 3). The actions to deceive and interfere with the processing of computer data with the objective of using false data or documents for relevant legal finalities is punishable with a maximum sentence of five years or 120 to 600 daily fines.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

The copying or dissemination of software protected by copyright law is punishable with a maximum sentence of three years' imprisonment or a fine under the Cybercrime Law.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The unlawful interception of data with the purpose of reproduction, selling or dissemination is punishable with a maximum sentence of three years' imprisonment or a fine.

Failure by an organisation to implement cybersecurity measures

The failure to implement appropriate cybersecurity measures is not a criminal offence in itself. However, the Portuguese supervisory authority, *Centro Nacional de Cibersegurança*, under the Cybersecurity Law (Law no. 46/2018), has inspection powers and may fine any organisation that fails to implement security measures.

Additionally, under GDPR, organisations are required to have in place the appropriate measures to prevent data breaches – taking into account the most recent technical developments, risks, the nature of personal data being processed and the damage to the rights and freedom of the data subject. The supervisory authority has inspection powers and may fine organisations that fail to implement the appropriate security measures for personal data.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The offences foreseen in the Cybercrime Law can be applicable to offences perpetrated by Portuguese citizens if no other law is applicable, to offences that are committed to the benefit of companies based in Portugal, offences committed in Portuguese territory or that are committed against IT systems in Portuguese territory regardless of where the offences are committed.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

There is no exception or mitigation to any penalty foreseen in the Cybercrime Law. However, the court can decide to mitigate any penalty under the general rules of the Criminal Code.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

When related to terrorism, cybercrimes have more severe penalties under the Anti-Terrorism Law (Law no. 55/2003, of August 22nd). Moreover, privacy intrusions through IT systems and swindling through computer data are criminal offences under the Criminal Code.

Additionally, other offences foreseen in the Criminal Code may apply, such as, for example, embezzlement, fraud or theft.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The Portuguese legal framework for cybersecurity is dispersed:

- the general legal framework for cybersecurity is Law no. 46/2018, August 13th – Cybersecurity Law – transposes the NIS Directive into Portuguese law;
- also applicable and complementing the NIS Directive, the Commission Implementing Regulation (EU) 2018/151 provides further requirements for digital service providers;
- in respect of cybercrime, complementing the Criminal Code, Law no. 109/2009, September 15th – Cybercrime Law – sets out cybercrime offences and communications surveillance and apprehension rules;
- the General Data Protection Regulation (GDPR) is applicable, when related to personal data, a new law, or when complementing the GDPR is being discussed, until enactment of the Data Protection Law (Law no. 67/98), which is also applicable;
- the Electronic Communications Law (Law no. 5/2004) is applicable to networks and services providers on electronic communications;
- also applicable, in respect to the identification and designation of critical infrastructures and the assessment of the need to improve their protection: Decree-Law no. 62/2011, May 9th;
- the Electronic Commerce Law is applicable to electronic services providers (Decree-Law no. 7/2004, January 7th amended by Decree-Law no. 62/2009, March 10th and Law no. 46/2012, August 29th); and
- the Portuguese competent authority and computer security Incident response team (national contact point for cybersecurity under NIS Directive) is *Centro Nacional de Cibersegurança* (CNCS), governed by Decree-Law no. 3/2012, January 16th, establishing the National Security Cabinet, amended by Decree-Law no. 69/2014, May 9th.

Also relevant is the National Strategy for Cybersecurity and Notice 459/2017, publishing the Portuguese Electronic Communications regulation for security and integrity of electronic communications networks and services.

Other legislation may apply with respect to civil and criminal matters.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Yes. In accordance with Law no. 46/2018, the NIS Directive transposition law, operators of critical infrastructures shall have in place technical and organisational measures to ensure the security of networks and information systems. These measures should ensure a level of security proportional to the risks and take into account the latest technical advances.

Portuguese law does not impose further requirements than those in the NIS Directive.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The organisations that provide electronic communication services must adopt not only monitoring, detection, prevention and mitigation Incidents, and business continuity plans. The regulator might establish the following measures:

- a permanent point of contact;
- a map of all the technical and organisational measures;
- evaluation exercises and drills; and
- an Annual Report.

Electronic service providers must retain one year's worth of electronic traffic and device location. Even though the courts recognise cases C 293/12 and C 594/12 (*Digital Rights Ireland*) the constitutional court, in 2017, ruled that the Portuguese law confers all the necessary guarantees required by the ECJ in order to guarantee the proportionality of the retention.

Public organisations, critical infrastructures and digital providers must ensure an adequate security level, considering the risk at stake and the technical progress, in order to reduce the risk of Incident, minimise impacts, ensure business continuity and to notify the competent authorities and evaluate the Incident's impact.

Digital providers must take into consideration:

- system and facilities' security;
- Incident management;
- business continuity management;
- auditing, tests and monitoring; and
- compliance with international standards.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

The Applicable Laws are largely harmonised at an EU level, and, as such, the risk of conflicts of laws is minimised.

The identified requirements have exceptions in the applicable data protection and fundamental rights legislation, and the courts have evaluated the proportionality of such measures regarding such fundamental rights.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Public organisations, critical infrastructures, digital providers and electronic service providers must notify any Incident with impact on the provision of its services to *Centro Nacional de Cibersegurança,* reporting, at least, the Incident's duration, the number of users affected, the geolocation of affected areas, level of severity of the Incident and impact of the economic and social activities.

Such notification does not imply any further responsibilities to the notifying party. Only substantial Incidents should be notified.

Should the Incident relate to Personal Data, the regulator, *Comissão Nacional de Protecção de Dados*, should be notified, if such Incident has an impact for the Data Subject's rights. Such notification should include the Incident's duration, the number of users affected, the data subject's rights affected and impact on the same and mitigation measures.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

This is not applicable.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Should the Incident relate to personal data, the data subject should be notified, if such Incident has a relevant impact on the data subject's rights. Such notification should include the Incident's duration, the number of users affected, the data subject's rights affected and the impact on the same and mitigation measures.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Please see questions 2.5 and 2.7.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Regarding public organisations, critical infrastructures and digital providers, the relevant regulator is *Centro Nacional de Cibersegurança*, a national authority with headquarters at Rua da Junqueira 69, 1300-342 Lisbon; email: cncs@cncs.gov.pt / telephone number: +351 210 497 400.

Regarding the provision of Electronic Communications, the relevant authority is ANACOM, with headquarters in Av. José Malhoa, 12; 1099-017 Lisbon; email info@anacom.pt / telephone number: +351 800 206 665.

Regarding Incidents with an impact on personal data, the relevant authority is *Comissão Nacional de Protecção de Dados* with headquarters in Av. D. Carlos I, nº 134, Lisbon; email: geral@cnpd.pt / telephone number: +351 213 928 400.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Regarding public organisations, critical infrastructures and digital providers not complying with the regulation, this might lead to a fine, which can range from €1,500 to €50,000 depending on the knowledge and intent of the parties.

Regarding the provision of electronic communications services, not complying with the regulation might lead to a fine which can range from €100 to €5,000,000, depending on the knowledge, size of the company, intent of the party and provision at stake.

Regarding personal data not complying with the regulation, this might lead to a fine under the terms of the GDPR (up to €20,000,000 or 4% of the company's or group's global turnover).

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The abovementioned requirements, with the exception of the electronics communication regulation, are part of a new legal framework; thus enforcement decisions are scarce.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The Portuguese Cybersecurity Law does not impose specific security measures depending on business sectors, except those already mentioned.

However, some industries are more prone to invest in information security, having dedicated teams. The financial services sector, the media sector and the sports sector, for example, have shown a growing concern for the implementation of further measures to prevent, detect, mitigate and respond to Incidents.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The Electronic Communications Law imposes specific technical and organisational measures, reporting obligations to national authorities and national security requirements to electronic communications networks providers and/or electronic communications services providers.

The regulator for financial services might impose some specific legal requirements in relation to cybersecurity, even imposing compliance with standard norms; for example, regarding measures concerning methods of payment on a case-by-case basis.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

The directors of a company have a general duty of care (duty to monitor) (article 64 of the Commercial Companies Code). This duty of care (duty to monitor) might concern a director's duty to prevent, mitigate, manage or respond to an Incident. The Commercial Companies Code, in case of a breach, allows for the director to be liable for damages caused by acts or omissions.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Even though ISO/IEC 27001, the ITIL and COBIT 5 frameworks are frequently used as standards for organisations to implement their own information security management systems, as well as provide some general guidance on the CISO framework organisational structures, there is still a mediocre practice of adopting a CISO, which is mainly directed at large companies. Currently, there is no obligation to designate a CISO.

As mentioned in question 2.3, some organisations are required to: establish a written Incident response plan or policy; conduct periodic cyber risk assessments, including for third-party vendors; and perform penetration tests or vulnerability assessments.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

The only applicable disclosure requirements are those mentioned in question 2.5.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

There are specific requirements regarding the handling of classified information and its supporting systems, which might have an impact on cybersecurity requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Regarding an Incident, a civil liability action for damages may be brought under the general terms of the Portuguese Civil Code and the rules of the Code of Civil Procedure.

In order to obtain compensation from the responsible party or subcontractor for damages suffered by the plaintiff, the fact that caused them harm must be attributable to the defendant.

Furthermore, a person who suffers damage in relation to an Incident, caused by lack of action of the regulator, may bring an action claiming both for compensation and for the regulator to act.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

One example is the ruling of 14/12/2016 of the Portuguese Supreme Court of Justice on the process 1063/12.1TVLSB.L1.S1 regarding a civil action of a company against a bank after a "phishing" attack, where the bank paid a due compensation amounting to the value stolen through the Incident and to moral damages, having found that the bank had not undertaken all the necessary measures.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

There is potential liability in relation to an Incident, since there is, as mentioned above, a specific duty to maintain the safety of the information; accordingly, there is a claim for compensation if there is a breach in the duty of the defendant towards the plaintiff resulting in an injury.

However, the claims may vary according to the existence of a contractual relation and the type of torts (intentional torts, negligent torts and strict liability torts).

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. Under the Insurance Contract Law, only insurance contracts that cover i) criminal liability or administrative fines, ii) the risk of crimes against personal liberty (such as kidnapping), and iii) possession or transport of unlawful drugs are prohibited.

Cyber insurances are available on the Portuguese insurance market.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Please see the answer above.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The employer is generally free to establish rules of conduct for its employees through internal regulation.

However, considering the monitoring of the employees and the reporting of Incidents, several requirements should be met, namely: the employees should have previous knowledge of the monitoring; the monitoring should not occur as per finding employees' wrongdoing; and the control should not be continuous monitoring of the employees activities and should not have the purpose of evaluating the employee's performance. The monitoring should be random and not directed at a specific employee and the employer should grant all means for the employees to follow the established rules.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are currently no applicable labour laws limiting the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee.

However, in order for such reporting to be legally required, it should be established in the internal rules of conduct and the employees should be granted the means in order to fulfil such requirement. If the reporting is legally demanded, the employer could eventually sanction an employee who does not follow such instruction.

It is recommended for the employer, in order to legally demand the report, to provide confidentiality and safety measures for the reporting of Incidents or potential Incidents.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The laws which give investigative powers to both the regulators and to law enforcement to investigate an Incident, are, besides those already mentioned in question 2.1, the following:

- Law of Cybercrime (Law no. 109/2009, of September 15th).
- Portuguese Criminal Code.
- Anti-Terrorism Law (Law no. 52/2003 of August 22nd, in compliance with Council Framework Decision 2002/475/JHA of June 13th, with the following amendments: Rectif. 16/2003, of October 29th; Law no. 59/2007, of September 4th; Law no. 25/2008, of June 5th; Law no. 17/2011, of May 3rd; and Law no. 60/2015, of June 24th).
- Internal Security Law (Law no. 53/2008, of August 29th).

An example of attributed investigative powers is the interception of communications for criminal cases, and investigation of a crime committed by means of a computer system or for which it is necessary to collect evidence in an electronic format.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

The Judgment of the Constitutional Court no. 413/2015, which set aside the rule that allowed the Secret Information Services to access "metadata" as well as tax and banking information started a doctrinal debate on the limits of the investigative power.

On July 19, 2017, a law was approved in order to allow the Secret Information Services not only to access the information mentioned above, but also to intercept communications even if through covert actions, provided that they are duly supervised.

Even though such powers allow for law enforcement to access some equipment, or the data generated, there is no specific requirements for the implementation of backdoors.

Miguel Duarte Santos
Gouveia Pereira, Costa Freitas & Associados, S.P. R.L.
Palácio Sottomayor, Rua Sousa Martins 1, 6º Andar, 1050-217 Lisboa
Portugal

Tel: +351 21 312 1550
Email: miguel.santos@gpasa.pt
URL: www.gpasa.pt

Miguel is an associate lawyer at Gouveia Pereira, Costa Freitas & Associados, S.P. R.L. – GPA Law Firm, working in the areas of insurance, banking, finance and securities law regarding its data protection, cybersecurity and regulatory aspects.

He specialises in insurance and banking law, having several years of experience advising and representing insurance companies, claims representatives, insurance brokers, national and foreign, on the applicable supervisory and regulatory provisions AML, GDPR, consumer protection, complaints management, conclusion of distance contracts and other applicable legal and regulatory frameworks, including cybersecurity.

He has significant experience in assisting international companies on access to the Portuguese insurance market, namely on authorisation procedures via the freedom of establishment and the freedom to provide services rights, as well as on the relevant legal and regulatory provisions for the rendering of the insurance activity.

Miguel has also published several scientific papers on related areas.

Sofia Gouveia Pereira
Gouveia Pereira, Costa Freitas & Associados, S.P. R.L.
Palácio Sottomayor, Rua Sousa Martins 1, 6º Andar, 1050-217 Lisboa
Portugal

Tel: +351 21 312 1550
Email: sofia.pereira@gpasa.pt
URL: www.gpasa.pt

Sofia obtained a Law Degree from the Faculty of Law of the Portuguese Catholic University, in Lisbon, in 1992. Sofia has a Master's Degree in Commercial Law from the Faculty of Law of the Portuguese Catholic University, with a thesis on "Supplementary Cash Contributions in the Portuguese Companies' Law" (2002).

Sofia is Specialist Lawyer in Financial Law, recognised by the Portuguese Lawyers' Bar Association since 2007.

With almost 25 years of experience, Sofia has advised several clients in their daily operations, namely regarding cybersecurity and the corresponding regulatory framework and compliance.

Sofia participated in Portugal in (i) the study for the transposition, by the Member States, of Directive 98/26/EEC, (ii) the study for the harmonization of the legal framework applicable to direct debits (2003), and (iii) the study related to the legal framework applicable to European companies in the EU Member States.

GPA
ADVOGADOS
LAW FIRM

GOUVEIA PEREIRA, COSTA FREITAS & ASSOCIADOS
SOCIEDADE DE ADVOGADOS, S.P., R.L.

Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P. R.L. (GPA) is an independent law firm with its head office in Lisbon whose mission is "Teaming with our Clients". In fact, it is GPA's commitment and concern to build and maintain a lasting relationship with its clients, becoming another member of their team.

GPA's team of lawyers provides specialised counselling in all the main areas of law, namely Corporate, Mergers and Acquisitions, Data Protection and Cybersecurity, Insurance, Banking, Finance, Public Law, Real Estate, Tourism, Labour, Oil & Gas and Litigation, allowing the firm to render a rigorous multidisciplinary service based on professional excellence.

With more than 80 lawyers and with offices in Lisbon, Algarve and Madeira, GPA has created the GPA Network, a network of law firms with offices in all the district capitals of Portugal, also being present in Angola, Cape Verde, Mozambique and São Tomé and Príncipe.

Romania

Silvia Uscov

Tudor Pasat

USCOV | Attorneys at Law

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Hacking constitutes a felony according to Article 360 of the Romanian Criminal Code as "Illegal access to a computerised system". The regulation sets different term ranges of imprisonment depending on the circumstances of the illegal actions, such as:

a) for the base form of the unlawful act, the penalty may consist in either a fine, or imprisonment ranging from three months up to a maximum of three years;

b) if the illegal actions are conducted with the purpose of gathering specific data from the system, the punishment consists of imprisonment for up to five years; and

c) presuming the access to the system is conditioned by various procedures, devices or specific programs, breaching this kind of system is punishable with imprisonment for up to seven years.

Moreover, Article 361 punishes the illegal interception of any confidential data information transfer from a computerised system with imprisonment from one to five years.

Denial-of-service attacks

Denial-of-service attacks incrimination may vary, due to aggravation causes or other objective incidental facts.

Article 362 of the Criminal Code states that it is punishable to illegitimately conduct the constraint of access to a computer system, which carries a sentence of imprisonment for one to five years.

Also, Article 363 of the same legislative act emphasises the importance of proper functioning of the system; therefore, a serious disturbance in a computerised system under the conditions of the previously mentioned article generate a higher liability of imprisonment, with a maximum term of seven years.

Moreover, the criminal legislation in force distinctively punishes denial-of-service attacks under two specific conditions: if the offender seeks a patrimonial benefit; and the existence of damage to the victim's detriment (Article 249).

Phishing

There is no provision precisely targeting phishing activity as a distinct felony, though it may fall within the scope of other regulations, such as Article 365 of the Criminal Code.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Such actions are prohibited by the Romanian legislation, depending on the purpose or the effects of the malware's infection of the system.

Therefore, in case of ransomware infection, the conduct may be qualified as mentioned above, based on Article 249.

Trojans and other viruses are covered by Article 362 and Article 363, mentioned above.

Spyware infection of an IT system may fall within the scope of Article 364, which punishes the illegal transfer of data information with imprisonment ranging from one to five years.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

The Criminal Code incriminates in its Article 365 the possession of hacking devices, passwords and any other information with the purpose of committing any cybercrime covered by the Romanian legislation. The punishment may consist in a fine or imprisonment for three months to two years.

Identity theft or identity fraud (e.g. in connection with access devices)

According to Article 327, identity fraud is punishable only if the offender's conduct targets a public authority, punishable with up to three years' imprisonment. Identity fraud may take the form of identity theft in the case of using the real identity of a certain individual, which leads to a punishment of up to five years' imprisonment.

Also, Article 325 punishes "Computerised Fraud", which is defined as the conduct of altering data information or restricting access to information with the purpose of producing unlawful legal consequences, punishable with imprisonment for one to five years.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

The legislation in force does not incriminate electronic theft as a stand-alone felony.

However, Articles 190 to 199 of Law no. 8/1996 regarding copyright cover a series of misdemeanour or felonies related to copyright infringement. For example, the punishment for piracy consists in imprisonment for six months to three years or, in case of commercial use, for two to seven years.

Any other unlawful use or distribution of work protected by copyright shall be punished with either a fine or imprisonment for one month to five years.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The Criminal Code punishes the theft of communication infrastructure, qualifying it as aggravated theft, punishable with imprisonment for three to 10 years (Articles 229 and 228).

Failure by an organisation to implement cybersecurity measures

Failure to implement cybersecurity measures is not considered to be a criminal offence, but an administrative one. Article 52 of Law no. 161/2003 regarding measures for transparency guarantees regarding the official's performance sets up a penalty consisting in a fine of up to 5,000 RON. This legislative act has been modified several times, but the Parliament did not take into consideration the currency revaluation that took place in the Romanian jurisdiction in 2005, so the fine limit is listed as 5,000,000 RON, which does not reflect reality.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Every criminal offence is liable to punishment according to the Romanian legislation in any of the following circumstances:

- the offender is a Romanian citizen or a legal person registered in Romania, no matter the territory the crime has been committed in, and the punishment for the crime is imprisonment for not less than 10 years. Otherwise, double jeopardy is necessary;
- the victim of the criminal offence is a Romanian citizen, a legal person registered in Romania, or a Romanian state authority;
- the offender is in Romania of his own free will and has committed a crime which the Romanian state is bound to address, according to an international treaty; and
- in any case in which the offender acted in the territory of Romania or the final result of the offence occurred in the same territory.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The Criminal Code stipulates a set of mitigating circumstances that may apply to any of the offences mentioned in question 1.1. Article 75 sets up two kinds of mitigating circumstances: legal circumstances; and judicial circumstances, the main difference between these two kinds being the fact that legal circumstances are compulsory in terms of application.

Even so, regarding the legal type of circumstances, it is hard to believe that they will ever be applicable to cybersecurity crimes (e.g. legitimate defence, necessity status).

Therefore, only judicial circumstances are applicable, such as the efforts conducted by the offender in order to diminish the consequences of his illegal conduct, or the existence of impartial circumstances liable to reduce the severity of the conduct imputable to the criminal.

The effect of the presence of judicial mitigating circumstances reflects upon the punishment, which would be reduced by ⅓ of the initial punishment established by the court.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

There are a few other felonies prescribed by legislation that may interfere with cybersecurity offences.

Article 250 punishes unlawful, fraudulent financial operations conduct with imprisonment for two to seven years. Moreover, as a distinct felony, Article 251 states that the acceptance of these fraudulent operations is punishable with imprisonment for up to five years. These offences may interfere with cybersecurity felonies, due to obvious reasons, fraudulent operations usually being conducted through computerised systems.

In terms of information classified as public, there are several provisions that may relate to cybersecurity matters, such as: Article 303 regarding disclosure of information classified as a state secret; or Article 304, which incriminates disclosure of any work-related secret information (disclosure of information classified as a service secret or not public) and information that is not destined for public knowledge. Also, Article 305 punishes negligence in storing information leading to information alteration or withdrawal. These provisions apply in the public administration sector.

Also, cybersecurity crimes may occur in tandem with another type of illegal conduct prohibited by Article 367 of the Criminal Code, entitled "Creation of an organised crime group", with a punishment of imprisonment for one to five years and prohibition of rights usage.

Moreover, all of the offences mentioned above may be retained by the court as inchoate.

A case of worldwide notoriety is Mihai Gheaţă's trial for conducting computerised fraudulent activity, punished by Article 249 of the Criminal Code, within an organised crime group made up of 31 other criminals. He has been also charged for hacking the Bank of America's database in 2004, creating a material damage of $3,000,000. Taking into consideration all his illegal activity, the Bucharest Court of Law sentenced him to 10 years in prison.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The main regulations covering cybersecurity offences are:

1) the Criminal Code of 17 July 2009;
2) Law no. 161/2003 regarding the Prevention and Punishment of Corruption;
3) the Budapest Convention on Cybercrime of 2001;
4) Law no. 535/2004 regarding the Prevention and Control of Terrorism; and
5) Law no. 8/1996 regarding Copyright and Other Connected Rights.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The Romanian Parliament passed Draft Law no. 280/2018 regarding the transposition of the Network and Information System Directive 2016/1148, yet the Constitutional Court has declared that the provisions of the act in question are against the Romanian Constitution.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

According to Law no. 161/2003, organisations are required to:

1) conduct activities regarding cybercrime prevention;
2) promote security policies, measures and standards targeting computerised systems;
3) organise information campaigns regarding cybersecurity crimes and the risks that the users are exposed to; and
4) inform users about the confidentiality and legal access conditions of the systems they administrate.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Due to the fact that Romania missed the transposition deadline of the Network and Information System Directive 2016/1148, the European Act in question is directly applicable.

The Directive goes into detail while stating the responsibilities each state has in order to maintain cybersecurity standards. For example, each state must designate a response team in case of Incidents and appoint a unique contact terminal with the purpose of international collaboration.

The Romanian law in force does not interfere with the Network and Information System Directive 2016/1148, but its enforcement must be done in compliance with the European Act under discussion. Even so, conflicts may arise regarding extraterritorial application of foreign laws.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There is an assembly of institutions with powers in cybersecurity supervising, according to Government Decision 271/2013, called the National Cybersecurity System. The most important body of the authority mentioned is the National Cybersecurity Alert System, whose main purpose is to prevent, report and overcome any potential Incident.

The Network and Information Systems Directive states that a Cooperation Group must be established, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security, with the purpose of facilitating the communication of Incidents between the authorities in power designated by each state.

In Romania, the authorities responsible for cybersecurity are:

1) the National Cybersecurity System, the most important body of this institution being the National Cybersecurity Alert System; and
2) the National Supervisory Authority for Personal Data Processing.

Moreover, the Security Incidents Response Team should receive notifications of Incidents, given the fact that its main purpose is to manage and solve them.

Any threat regarding the security and proper functioning of the computerised system triggers the obligation to report the Incident, with the purpose of ensuring the integrity of the data system.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

The Government Decision mentioned above encourages the organisations to cooperate by any means in order to prevent any Incident.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Regulation (EU) 2016/679 states that any organisation must inform the authority in power – the National Supervisory Authority for Personal Data Processing – about the data security breach within 72 hours after having become aware of the situation, unless the Incident is unlikely to result in a risk to the rights and freedoms of natural persons.

According to the Network and Information Systems Directive, reporting Incidents may also be directed to the Response Team or other authorities in power, such as the National Cybersecurity Alert System.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Essentially, the responses would not change because the information exchange between authorities relies on a legal basis. The primary

purpose of this exchange is to protect the vital interests of any person affected by the Incident.

By way of exception, regarding special categories of personal data mentioned by Regulation (EU) 2016/679 (General Data Protection Regulation), the explicit consent of the affected individuals is required.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

There are several authorities in charge of law enforcement regarding cybersecurity:

1) the Romanian Intelligence Service, which is responsible for monitoring the integrity and safety of computerised systems, due to the fact that felonies against these values may be considered acts of terrorism;
2) the Ministry of Communication and Informational Society, which coordinates the National Cybersecurity and Incident Response Team mentioned in question 2.7;
3) the Supreme Defence Council created by the authorities mentioned in question 2.5; and
4) the National Supervisory Authority for Personal Data Processing.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Under Romanian law, non-compliance may result in applying administrative fines up to 5,000 RON.

Non-compliance with Regulation (EU) 2016/679 (General Data Protection Regulation) is subject to an administrative fee of up to 10,000,000 EUR or 2% of the total worldwide annual turnover, whichever is higher.

Moreover, Article 251 of the Criminal Code states that the acceptance of fraudulent operations is punishable with imprisonment for up to five years.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The National Authority for Supervising Personal Data Processing has punished several personal data controllers for not complying with the law in force, such as S.C. Vodafone Romania S.A., which was fined 10,000 RON for not taking all the technical measures to ensure the personal data protection of its customers.

Another company, S.C CETELEM IFN S.A., refused to provide the relevant authority with the required information and conducted illegal data processing. This conduct resulted in a fine of 35,000 RON.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practice in terms of information security is not unitary and the prevention, detection or any other measures may vary, depending on the business sector. Therefore, market sectors that process sensitive information will invest more in software, infrastructure and human resources. Even so, there are no special provisions regarding any specific sectors.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Both sectors follow the common rules of Regulation (EU) 2016/679 (General Data Protection Regulation).

However, the telecommunications sector is required to deploy any necessary measures in order to handle any Incidents. Annually, the National Authority for Management and Regulation in Communications of Romania sends a report regarding the measures taken to the European Commission and to the European Union Agency for Network and Information Security.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

First of all, the responsibility of the company may not encroach on the liability of the shareholders for the share capital each one of them owns.

Moreover, each company's General Assembly will appoint an administrator/a Board of Directors responsible in any matter regarding the functioning of the company. Therefore, it is the administrator's duty to respond, through the company's bodies designated for managing the Incidents, and act purposefully in preventing, managing and mitigating Incidents. In this regard, Law no. 31/1990 states in its Article 73 that the managing body, which may consist of an administrator or a Board of Directors, is responsible and is severally liable for the execution of the legislative requirements.

The legislative act mentioned above does not set special provisions on this matter with criminal implications, the Romanian Criminal Code being the reference legislative act, and the felonies that may arise already having been provided for.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

According to the legislation in force and Regulation (EU) 2016/679 (General Data Protection Regulation), both listed and private companies are required to designate a chief information security officer, to establish an Incident response plan or policy and to conduct periodic cyber risk assessments.

Regarding penetration tests and vulnerability assessments, they may be conducted in connection with cyber risk assessments, though they are not specifically required by law.

The Network and Information Systems Directive 2016/1148 states that companies should take all the measures necessary to manage any data breach risk. Moreover, companies should alert the relevant authorities and the Computer Security Incident Response Team (CSIRT) as soon as possible. In this case, companies should alert the National Cybersecurity Alert System and the National Authority

for Supervising Personal Data Processing (according to General Data Protection Regulation).

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Generally, no specific disclosure requirements are required, except those covered by the General Data Protection Regulation. Also, please see the answer to question 3.2.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

There are no further provisions worth mentioning besides those already discussed.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The Romanian Civil Code provides two different cases in which civil actions may be put into use.

First of all, liability in tort may be triggered, under the general requirements stated by the Civil Code. Please see the answer to question 5.3.

Also, civil actions can be triggered based on contractual liability. Contractual liability implies the existence of a set of special clauses inserted in the contract that mention any obligations of the company facing the Incident. Therefore, the aggrieved party to the contract may initiate proceedings against the company under the regulations set forth in the contract.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

The case law on Incidents lacks notable examples, due to the fact that both Regulation (EU) 2016/679 (General Data Protection Regulation) and the Network and Information System Directive 2016/1148 are novel elements in the Romanian legislation, and no remarkable Incidents have been recorded thus far.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

As mentioned before, yes, in theory it is possible for liability in tort to be triggered in case of an Incident.

Even so, there is a set of requirements that each Incident must meet in order to inflict the liability in tort:

a) the Incident must be a consequence of a legislative violation;

b) the illicit conduct must produce material or moral damage at the expense of the victim;

c) the individual called upon to remedy the damage must have committed the acts with the guilt required by the law for the legislative breach in question; and

d) there must be a causal link between the damage done and the illicit actions of the culpable individual.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Organisations are permitted to take out insurance against possible Incidents.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no specific regulations regarding the limitations to insurance coverage; therefore, companies providing these services have the right to establish thresholds freely.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

Generally, by signing the employment contract the employee consents to personal data processing. The employer can monitor and use the data provided in the workplace under certain conditions:

1) the existence of a legitimate interest from the employer; and

2) compliance with the principle of proportionality.

Moreover, the National Authority for Supervising Personal Data Processing stated that the monitoring of employees must be done with the prior knowledge of the employees. Also, the employees must explicitly consent to the work conditions related to their monitoring.

There are no specific provisions that may require the employee to report any cyber risks, and so employers should stipulate such obligations in their contracts/internal policies.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

The Romanian legislation in force provides a set of principles to follow while reporting any misleading conduct. The principles are set up in order to protect the proper functioning of the authorities, and not necessarily to limit the initiative of the employees in proceeding with such a report.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

There are several authorities with different investigatory powers granted by the current legislation.

The Ministry of Communication and Information Society, the Romanian Intelligence Service and the Organised Crime and Terrorism Investigation Directorate have general investigatory powers in relation to cybersecurity matters.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There is no such explicit legal requirement. However, given the general rules of data protection diligence, backdoor activities may contribute to safer system maintenance.

Silvia Uscov
USCOV | Attorneys at Law
23 Titus Street
Bucharest 4
Romania

Tel: *+40 745 947 310*
Email: *silvia.uscov@uscov.eu*
URL: *www.uscov.eu*

Silvia Uscov is a Managing Partner of USCOV | Attorneys at Law, overseeing the Bankruptcy and Restructuring workgroup. As an experienced business attorney, she draws on her experience in corporate law, commercial and business crime litigation. An experienced human rights lawyer, Silvia has safeguarded human rights and civil liberties through civil and criminal proceedings, in front of both local and international courts such as ECHR.

Through her practice, Silvia has taken to the bar in various business crime cases involving prosecution by specialised criminal investigation units against both business owners and executive employees. Combining commercial and business law expertise with a productive white-collar defence career, she can effectively represent complex interests of both companies and their executives.

Silvia has an M.A. (Criminal Law), a diploma in International Relations from the Romanian Diplomatic Institute (Ministry of Foreign Affairs), and is a graduate of the Law School of the University of Bucharest.

Tudor Pasat
USCOV | Attorneys at Law
23 Titus Street
Bucharest 4
Romania

Tel: *+40 787 532 600*
Email: *tudor.pasat@uscov.eu*
URL: *www.uscov.eu*

Tudor Pasat has been working within USCOV | Attorneys at Law as a paralegal since 2018.

His main activity concerns various domains, such as mergers and acquisitions, company incorporation, intellectual property, criminal law and its commercial implications, administrative law, and real estate.

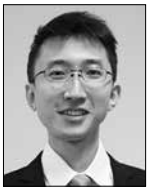
Before joining USCOV | Attorneys at Law, Tudor took part in different internship programmes, most of them being undertaken at some of the finest law firms.

He is a native speaker of Romanian and fluent in English.

Chapter 28

Singapore


Rajesh Sreenivasan


Michael Chen

Rajah & Tann Singapore LLP

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

According to the applicable legislation specified below, the following activities would constitute criminal offences in Singapore.

Hacking (i.e. unauthorised access)

Yes. Under section 3 of the CMA, any person who knowingly causes a computer to perform any function for the purposes of securing access without authority to any program or data held in any computer shall be guilty of an offence.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding two years, or to both.

In *Public Prosecutor v Muhammad Nuzaihan bin Kamal Luddin* [1999] 3 SLR(R) 653, the accused relied on an exploit, instead of sophisticated software, to perform unauthorised access to an internet service provider server, among others. In *Lim Siong Khee v Public Prosecutor* [2001] 1 SLR(R) 631, the accused hacked the victim's email account by answering correctly the hint question to successfully retrieve passwords and to gain unauthorised access. He was sentenced to 12 months' imprisonment.

Denial-of-service attacks

Yes. Under section 7 of the CMA, any person who knowingly and without authority or lawful excuse (a) interferes with, interrupts or obstructs the lawful use of a computer, or (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in computer, shall be guilty of an offence.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years, or to both.

There have been no prosecutions for denial-of-service attacks as yet. Nevertheless, such attacks are recognised as threats under Singapore's Cybersecurity Strategy.

Phishing

There is no specific provision that deals with phishing. However, under section 3 of the CMA, any person who knowingly causes a computer to perform any function for the purposes of securing access without authority to any program or data held in any computer shall be guilty of an offence.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding two years, or to both.

In July 2018, there was a prosecution relating to multiple phishing activities, and it was reported that the offender was sentenced to three years and five months' imprisonment, and fined S$5,000.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. Under section 5 of the CMA, a person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years, or to both.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Yes. Under section 8B of the CMA, it is an offence for a person to obtain or retain any item (which includes hacking tools, among others) with the intent to use it to commit or facilitate commission of an offence under the CMA.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years, or to both.

Identity theft or identity fraud (e.g. in connection with access devices)

Yes. Under section 4 of the CMA, it is an offence to secure unauthorised access to any computer program or data, with the intent to commit an offence involving property, fraud or dishonesty. This offence is punishable on conviction by a fine not exceeding S$50,000 or imprisonment for a term not exceeding 10 years, or to both.

In *Public Prosecutor v S Kalai Magal Naidu* [2006] SGDC 226, the accused was convicted under section 4 for conducting searches on her bank employer's computer systems to effect cash withdrawals from the victim's bank account. She was sentenced to four months' imprisonment for each charge under section 4.

Also, under section 5 of the CMA, an accused may be charged for unauthorised modification of computer material. This may be seen in *Public Prosecutor v Tan Hock Keong Benjamin* [2014] SGDC 16, where the accused used the victim's debit card that he found to make a purchase on eBay. It was held that he knew that by doing so, he would cause unauthorised modification to the contents of a computer, namely the data stored in the bank's servers, such that the online purchase would be approved.

In addition, the Penal Code contains provisions on cheating by personation. Although not cyber-specific, section 416 of the Penal Code (cheating by personation) may apply to identity theft. It is an

offence for anyone to cheat by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is. The punishment is imprisonment for a term which may extend to five years or a fine, or both.

Under section 170 of the Penal Code, it is an offence to personate a public servant. The punishment is imprisonment for a term which may extend to two years or a fine, or both.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Yes. Under section 8A of the CMA, it is an offence for a person to obtain or retain personal information, or to supply, offer to supply, transmit or make available the personal information, if the person knows or has reason to believe that any personal information about another person (being an individual) was obtained by an act done in contravention of the CMA. This offence is punishable on conviction by a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years, or to both.

The theft of personal data could constitute an offence under the PDPA. Under section 51 of the PDPA, it is an offence for an organisation or individual to dispose of, alter, falsify, conceal or destroy personal data. The punishment for this offence is a fine of up to S$5,000 in the case of an individual, and up to S$50,000 in any other case.

Under section 136 of the Copyright Act, the following instances of copyright infringement are criminal offences, where the infringing party knows or ought reasonably to know that the copies are infringing ones: make for sale or hire infringing copies; sell or let for hire infringing copies; possess or import infringing copies for commercial purposes; and distribute infringing copies for commercial purposes.

There is also criminal liability if the copyright infringement is wilful and either or both of the following two situations apply: (i) the extent of the infringement is significant; and/or (ii) the person does the act to obtain a commercial advantage.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Under the CMA, it is an offence to perform unauthorised use or interception of a computer service (section 6), and for unauthorised disclosure of an access code (section 8). Attempts are also caught under section 10 of the CMA, whereby anyone who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under the CMA shall be guilty of an offence. Therefore, any forms of attempts to gain unauthorised access, or to commit any other offences under the CMA, will constitute offences as well.

Failure by an organisation to implement cybersecurity measures

The PDPA requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. If the organisation does not comply with this requirement, the Personal Data Protection Commission (the "**PDPC**") can give the organisation directions to ensure compliance; for example, directing the organisation to pay a financial penalty of up to S$1 million.

The Cybersecurity Act 2018 (No. 9 of 2018) requires owners of designated critical information infrastructure ("**CII**") to audit the compliance of their CII with the Cybersecurity Act and the applicable codes of practice and standards of performance at least once every two years, and conduct a cybersecurity risk assessment of the CII at least once a year. Any CII owner which does not comply shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding two years, or to both.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The CMA, PDPA and Penal Code have extraterritorial application. The Cybersecurity Act applies to any CII located wholly or partly in Singapore. Section 11 of the CMA specifies that the CMA provisions have effect against any person, irrespective of nationality or citizenship, even if the person is outside or within Singapore, if:

(a) the accused was in Singapore at the material time of the offence;

(b) the computer, program or data was in Singapore at the material time of the offence; or

(c) the offence causes or creates significant risk of serious harm in Singapore.

The above captures anyone who commits an offence under the CMA for which the person targets a computer, program or data located in Singapore, or if the person was located in Singapore when the offence happened. Also, if the offence causes significant risk of serious harm in Singapore, then the extraterritorial provision may apply. Examples of serious harm include the disruption or serious diminution of public confidence in essential services such as communications and transport infrastructure or public utilities.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The legislation does not specify mitigating factors to the above offences. Nevertheless, cooperation with the relevant regulators or enforcement authorities, or active steps taken to mitigate the loss or damage caused by any of the offences, could be viewed by a court as mitigating factors.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

In addition to legislation specifically targeted at cybercrime, the existing criminal offences as set out in the Penal Code and Sedition Act (Cap. 290), among others, may be able to encompass offences relating to cybersecurity. It is generally an offence (even though not specific to cybersecurity) to commit or facilitate terrorism activities, e.g., where there is financing of terrorism.

The Protection from Harassment Act (Cap. 256A) (the "**POHA**") establishes that it is an offence to intentionally cause harassment, alarm or distress, and to commit unlawful stalking. For example, unlawful stalking includes keeping the victim or a related person under surveillance.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The current laws which relate to cybersecurity in Singapore include:

Cybersecurity Act 2018 (No. 9 of 2018)

The provisions of this Cybersecurity Act relating to CII came into operation on 31 August 2018. The Cybersecurity Act establishes a framework for the oversight and maintenance of national cybersecurity in Singapore, and imposes duties and obligations on owners of CII.

Computer Misuse Act (Cap. 50A) (CMA)

The CMA sets out penalties for various cybersecurity offences, as described in section 1 above. Depending on the offence, the maximum quantum of the fine ranges from between S$5,000 to S$50,000, and the maximum imprisonment term ranges from between two and 10 years. The penalties may be enhanced in specific circumstances. For example, the maximum fine quantum and imprisonment term are increased in the case of second or subsequent convictions.

Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA)

The PDPA imposes data protection obligations on private organisations when they perform activities involving the collection, use and disclosure of personal data. The PDPC has powers to bring enforcement actions against organisations which fail to comply with these PDPA obligations.

Penal Code (Cap. 224)

As described in section 1 above, the Penal Code sets out offences relating to personation, among others.

Copyright Act (Cap. 63)

As described in section 1 above, the Copyright Act establishes that certain acts of copyright infringement constitute offences.

Strategic Goods (Control) Act (Cap. 300)

The Strategic Goods (Control) Act controls the transfer and brokering of strategic goods and strategic goods technology (including specified information security and cryptographic systems), among others.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

In the Cybersecurity Act, there are cybersecurity requirements that impose duties on owners of CII. Per the Act, CII refers to a computer or computer system that is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore. The Commissioner will have the power to designate a computer or computer system as a CII.

'Essential services' are specified in the First Schedule of the Act. The First Schedule details 46 types of services which may be considered as 'essential services', under the broad categories of energy, info-communications, water, healthcare, banking and finance, security and emergency services, aviation, land transport, maritime, Government, and media.

Section 9 of the CMA enhances the punishment for certain offences that are committed on protected computers (including computers used for defence, communications, public utilities, and banking, among others). The applicable punishment is increased to a maximum fine of up to S$100,000, and/or imprisonment for a term not exceeding 20 years.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the Protection Obligation imposed by the PDPA, an organisation is required to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Under the Cybersecurity Act, CII owners will be required to: comply with such codes of practice, standards of performance, or directions in relation to the CII as may be issued by the Commissioner; carry out regular audits and risk assessments; and participate in cybersecurity exercises as required by the Commissioner.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

No such issues have been reported to have arisen thus far in Singapore.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

The PDPA does not contain a mandatory reporting obligation. However, the PDPC has issued non-binding guidelines recommending organisations to voluntarily notify the PDPC as soon as possible of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals.

The PDPC is currently reviewing the PDPA, and issued a public consultation (from 27 July 2017 to 21 September 2017) seeking feedback on its proposed amendments. In February 2018, the PDPC issued a response to the feedback received from the public consultation. One amendment relates to mandatory data breach notification. In the PDPC's response, it is proposed that organisations must:

(a) notify the affected individuals and PDPC if a data breach is 'likely to result in significant harm or impact to the individuals to whom the information relates'; or

(b) notify the PDPC if there is a 'significant scale of breach' (but there will not be a statutory threshold as initially proposed).

The Cybersecurity Act imposes a duty on CII owners to report cybersecurity Incidents to the Commissioner of Cybersecurity if these Incidents involve CII or systems interconnected with CII. The information required for reporting (and corresponding time limits) are prescribed by the Commissioner, and include the nature, cause, and impact of the Incident, and the remedial measures taken.

The Cybersecurity Act also grants the Commissioner powers to investigate all cybersecurity threats and Incidents (not only those involving CIIs); for example, to obtain information (such as technical logs), and, in the event of serious cybersecurity threats and Incidents, to enter premises where relevant computers and computer systems are located, access such computers, and scan computers for cybersecurity vulnerabilities. In addition, the Commissioner will be empowered to direct any person or organisation to take emergency measures and requirements to prevent, detect or counter any threat to essential services or the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

While there are no general restrictions with regards to voluntary sharing of information pertaining to an Incident, this is subject to sector-specific regulations and regulatory oversight which may constrain an organisation from sharing such information. If the information pertains to personal data, the organisation must comply with the PDPA in sharing such information. Additionally, organisations should not share information protected on the grounds of it being a national secret or which is prejudicial to national security, under the Official Secrets Act and Internal Security Act, respectively.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The PDPA does not contain a mandatory notification obligation. However, the PDPC has issued non-binding guidelines recommending organisations to voluntarily notify affected individuals immediately if a data breach involves sensitive personal data. Note that 'sensitive personal data' is not defined under the PDPA, only 'personal data'.

The PDPC is currently reviewing the PDPA, and has issued a public consultation (from 27 July 2017 to 21 September 2017) seeking feedback on its proposed amendments. One amendment relates to a mandatory data breach notification. It is proposed that organisations must notify the affected individuals and PDPC if a data breach is 'likely to result in significant harm or impact to the individuals to whom the information relates'. Based on the PDPC's response to the feedback, certain exemptions may apply to the notification requirement to affected individuals; for example, if notification is likely to impede investigations, or where the breached personal data is technologically protected.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, the responses do not change, provided that any PDPA requirements are complied with if the information includes personal data.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Regulators responsible for enforcing requirements are generally either sector-specific or subject matter-specific, including but not limited to:

Sector/ Subject Matter	Relevant Statute/Regulations	Regulators
Cybersecurity	Cybersecurity Act, CMA	MCI, CSA
Personal Data	PDPA	PDPC
Penal Offences	Penal Code	Singapore Police Force ("**SPF**")
Sector-Specific Regulations	Banking and Financial Sector Laws/Notices/Guidelines	Monetary Authority of Singapore ("**MAS**")
	Telecommunications Act	Infocomm Media Development Authority ("**IMDA**")

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Penalties for failure to comply with any of the abovementioned requirements are dependent upon the respective statutes, regulations or guidelines, for example:

- The PDPC has powers to issue directions and bring enforcement actions to ensure compliance with the PDPA. For example, the PDPC can impose a financial penalty of up to S$1 million.
- Under section 14 of the Cybersecurity Act, a CII owner who fails to notify the Commissioner of a prescribed cybersecurity Incident in respect of the CII within the prescribed period after becoming aware of such occurrence, shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding two years, or to both.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The PDPC has taken an active role in ensuring action be taken against organisations which breach the PDPA. By way of example, on 21 April 2016, the PDPC imposed financial penalties of S$50,000 and S$10,000 on K Box Entertainment Group ("**K Box**") and its data intermediary, Finantech Holdings, for failing to implement proper and adequate protective measures to secure its IT system, resulting in unauthorised disclosure of the personal data of 317,000 K Box members. K Box was also issued directions and penalised for the absence of a Data Protection Officer.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Apart from the PDPA requirement for all organisations to make

reasonable security arrangements to protect personal data, other cybersecurity obligations and requirements are imposed in sector-specific legislation, codes of practice, and guidelines, such that information security measures vary depending on business sector.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Financial services sector

Under the Technology Risk Management Notices, regulated financial institutions are required to notify the MAS as soon as possible, but not later than one hour, upon the discovery of a relevant Incident. Regulated financial institutions are required to submit a root cause and impact analysis report to the MAS, within 14 days or such longer period as the MAS may allow, from the discovery of the relevant Incident.

A 'relevant Incident' refers to a system malfunction or IT security Incident, which has a severe and widespread impact on the financial institution's operations or materially impacts the financial institution's service to its customers.

The MAS has also issued guidelines for financial institutions to mitigate cybersecurity risks, such as the Technology Risk Management Guidelines, Outsourcing Guidelines, Business Continuity Management Guidelines, and Bring-Your-Own-Device ("**BYOD**") Circular.

In September 2018, the MAS issued a public consultation regarding the Notice on Cyber Hygiene, regarding MAS' intention to issue a Notice on Cyber Hygiene, which prescribes a set of essential cybersecurity practices that financial institutions must put in place to manage cyber threats.

Telecommunications sector

The IMDA has formulated the Telecommunication Cybersecurity Code of Practice to enhance the cybersecurity preparedness for designated licensees. Besides security Incident management requirements, the Code includes requirements to prevent, protect, detect and respond to cybersecurity threats.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Failure by a company to prevent, mitigate, manage or respond to an Incident could amount to a breach of directors' duties; for example, if the failure results from a director's breach of their duty to act honestly and use reasonable diligence in the discharge of the duties of their office.

While not mandatory, the Code of Corporate Governance ("**Code**") sets out best practices in relation to corporate governance principles. The Code of Corporate Governance is issued by the MAS, on recommendation by the Corporate Governance Council, and was last revised on 6 August 2018. Under Principle 9 'Risk Management and Internal Controls', the board of directors is responsible for the governance of risk and should ensure that management maintains a sound system of risk management and internal controls, to safeguard the interests of the company and its shareholders.

In relation to financial institutions, the MAS has issued the Technology Risk Management Guidelines, which set out technology risk management best practices and recommend that, in view of the importance of the IT function in supporting a financial institution's business, the board of directors and senior management should have oversight of technology risks and ensure that the organisation's IT function is capable of supporting its business strategies and objectives. The board of directors and senior management should ensure that a sound and robust technology risk management framework is established and maintained. They should also be fully responsible for ensuring that effective internal controls and risk management practices are implemented to achieve security, reliability, resiliency and recoverability.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There is currently no general requirement under Applicable Laws for all companies to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments; and (d) perform penetration tests or vulnerability assessments.

Nevertheless, there are sector-specific cybersecurity requirements. For example, in relation to financial institutions, the MAS Technology Risk Management Guidelines recommend that financial institutions devise an Incident response framework, perform risk assessments, as well as penetration tests and vulnerability assessments. The MAS Outsourcing Guidelines recommend that financial institutions conduct periodic risk assessments on outsourced service providers, and review and monitor the security practices and control processes of the outsourced service providers on a regular basis.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Companies are currently not subject to specific disclosure requirements in relation to cybersecurity risks or Incidents (whether to listing authorities, the market or otherwise in their annual reports).

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Companies may be subject to specific cybersecurity requirements under sector-specific codes or guidelines, such as those set out in section 3 above.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

An Incident could give rise to claims in contract (for breach of contract) or tort (as set out under question 5.3 below).

The PDPA provides for a right of private action, whereby any person who suffers loss or damage directly as a result of a contravention of certain Data Protection Provisions by an organisation shall have

a right of action for relief in civil proceedings in a court. In such a private action, the court may grant the plaintiff all or any of the following: (a) relief by way of injunction or declaration; (b) damages; and/or (c) such other relief as the court thinks fit.

Under the CMA, the court may order a person convicted of a CMA offence to pay compensation to any victim of the offence. This order will not prejudice the victim's right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

There have not been reported cases directly relating to civil actions brought in relation to Incidents.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

A party may face potential liability in tort in relation to an Incident; for example: if the Incident results from the party's negligence; there is a breach of confidence; or there is a breach of statutory duties.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. Organisations are permitted to take out insurance against Incidents. Often known as 'cyber insurance', such insurance may cover business interruption loss due to network security failure or attack, human errors, or programming errors, among others.

As this type of insurance is relatively novel in Singapore, it has been reported that the MAS and CSA have been working with industry partners and a Singapore university to research on cyber risk, security and insurance, so as to develop insurance schemes to protect citizens and businesses against cyber attacks.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Currently, there are no regulatory limitations to insurance coverage against the specified losses, such as business interruption, system failures, cyber extortion or digital asset restoration.

Notwithstanding the above, the general rule of *ex turpi causa non oritur actio* applies to insurance contracts as it applies to contractual illegality. A person cannot rely on his own illegal act to make a claim against his insurance policy, nor benefit from his own criminal conduct. This is also contrary to public policy, since allowing the indemnification of such risks would be to encourage the commission of crimes, which would be wholly against public policy.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

(a) Generally, the Applicable Law does not impose specific requirements on employers to monitor employees for the purposes of preventing, detecting, mitigating and responding to Incidents.

In relation to financial institutions, the MAS Technology Risk Management Guidelines recommend that, for accountability and identification of unauthorised access, financial institutions should ensure that records of user access are uniquely identified and logged for audit and review purposes. The MAS recommends that financial institutions should closely supervise staff with elevated system access entitlements and have all their systems activities logged and reviewed as they have the knowledge and resources to circumvent systems controls and security procedures.

In the non-binding Advisory Guidelines issued by the PDPC, which provide examples of security arrangements to protect personal data, the PDPC recommends restricting employee access to confidential documents on a need-to-know basis.

(b) There are no requirements under Applicable Law regarding the reporting of Incidents or potential Incidents by employees to their employers. However, it is to be noted that under the employment contracts or internal company policies, there may be such notification requirements imposed upon employees.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are currently no Applicable Laws which may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

CMA: computer misuse offences are investigated by the SPF. More specifically, within SPF's Criminal Investigation Department, the Technology Crime Division conducts investigation and forensic examination into technology-related offences committed under the CMA. The SPF's powers of investigation are set out under the Criminal Procedure Code (Cap. 63) ("**CPC**").

PDPA: the PDPC can initiate investigations upon complaint or its own motion. It has the power to require relevant documents or information, and the power to enter premises without warrant as well as under warrant.

Internal Security Act ("**ISA**"): in the interest of Singapore's national security, the ISA provides for the Government's power to order preventive detention, and the power of police to search and seize subversive documents, among other powers.

Cybersecurity Act: the Act grants investigative powers to the Cybersecurity Commissioner (or any other cybersecurity officer upon his authorisation), and permits the exercise of powers necessary to determine the impact or potential impact of the cybersecurity threat or Incident.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Under section 40(2) of the CPC, for the purposes of investigating an arrestable offence, the Public Prosecutor may by order authorise a police officer or an authorised person to require any person, whom he reasonably suspects to be in possession of any decryption information, to grant him access to such decryption information as may be necessary to decrypt any data required for the purposes of investigating the arrestable offence. Failure to comply is an offence punishable by a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years, or to both.

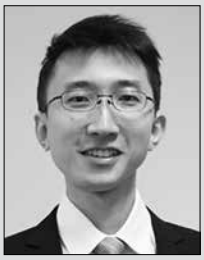
Under the Cybersecurity Act, the Minister for Communications and Information has the power to issue directions to any person or organisation to take such measures, such as the exercise of powers referred to under section 40(2) of the CPC to require decryption information, as may be necessary to prevent, detect or counter any serious and imminent cyber threat to essential services, national security, defence, foreign relations, economy, public health, public safety or the public order of Singapore.

Rajesh Sreenivasan
Rajah & Tann Singapore LLP
9 Battery Road #25-01
Singapore 049910
Singapore

Tel: +65 6232 0751
Email: rajesh@rajahtann.com
URL: sg.rajahtannasia.com

Rajesh Sreenivasan heads the Technology Media and Telecommunications Practice at Rajah & Tann Singapore LLP. He has been advising clients on matters relating to cybersecurity, data protection, telecommunications, electronic commerce, IT contracts, digital forensics and digital media for over 20 years.

His clients include financial institutions, state governments, multinational corporations in the telecoms, computer hardware and software sectors, government-linked companies and statutory boards. On the regional front, Rajesh has been engaged by the ASEAN Secretariat to facilitate a pan-ASEAN forum on legislative and regulatory reforms to collectively address convergence of IT, telecoms and broadcasting across all 10 member countries, and by the Commonwealth Secretariat to co-lead an e-government capacity building exercise involving all member Caribbean nations. Rajesh has also been the contributing author for the Singapore chapter of Sweet & Maxwell's *Data Protection Laws of the World* since 2010. Rajesh has been cited as a leading TMT lawyer by all major legal ranking directories.



Michael Chen
Rajah & Tann Singapore LLP
9 Battery Road #25-01
Singapore 049910
Singapore

Tel: +65 6232 0780
Email: michael.chen@rajahtann.com
URL: sg.rajahtannasia.com

Michael Chen is an Associate in the Technology Media and Telecommunications Practice at Rajah & Tann Singapore LLP. He has assisted in an extensive range of intellectual property, technology, media, and data protection matters. He actively advises on a wide range of technology contracts.

He graduated from the University of Melbourne Law School and is admitted in both Singapore and Australia. Michael has a keen interest in computers and technology, and also holds a degree in electrical and computer engineering from Cornell University.

South Africa

Fatima Ameer-Mia

Cliffe Dekker Hofmeyr Inc

Christoff Pienaar

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

At present, the current legal framework relating to cybercrime in South Africa is a hybrid of different pieces of legislation and the common law. Offences relating to cybercrime are primarily regulated under the Electronic Communications and Transactions Act 25 of 2002 ("**ECT Act**").

It has been recognised in South Africa that the current hybrid legal framework relating to cybercrimes and cybersecurity (in particular the common law, which develops on a case-by-case basis) has not kept up with the dynamic nature of technology and international standards. Accordingly, in September 2015, the first draft Cybercrimes and Cybersecurity Bill ("**Cybercrimes Bill**") was published in the South African parliament for comment. The most recent version of the Cybercrimes Bill [B6 of 2017] has recently been tabled in parliament but has not yet been promulgated into law.

The Cybercrimes Bill, once effective, will, *inter alia*, consolidate and codify numerous existing offences relating to cybercrime as well as create a variety of new offences which do not currently exist in South African law. The Cybercrimes Bill also deals with penalties for such cybercrime offences, provides for the powers of investigation, search, access and seizure in relation to prosecution of such offences, and regulates jurisdiction of the courts.

It is important to note that once the Cybercrimes Bill is in effect, it will repeal the relevant provisions in the ECT Act relating to cybercrime offences and cybersecurity.

We therefore set out the current legal framework below, as well as how this may differ under the pending legislation.

Hacking (i.e. unauthorised access)

Yes. Hacking is recognised as an offence under section 86(1) of the ECT Act, which states that it is an offence to intentionally access or intercept data without the appropriate authority of permission to do so. This also applies to unauthorised interference with data as contained in section 86(2) of the ECT Act. Under the ECT Act, the maximum penalty is a fine (unspecified) or imprisonment for a period not exceeding 12 months.

Under the Cybercrimes Bill, the offence of hacking is more broadly defined as it encompasses the unlawful and intentional access to data, a computer program, a computer data storage medium, or a computer system (section 2(1)). Under the Cybercrimes Bill, the maximum penalty is a fine (unspecified) or imprisonment for a period not exceeding five years (or both).

Denial-of-service attacks

Yes. Section 86(5) of the ECT Act states that any person who commits any of the acts described in sections 86(1)–86(4) with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.

For the sake of completeness:

- section 86(1) – see discussion above in relation to hacking;
- section 86(2) – criminalises the unlawful intentional interference with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective;
- section 86(3) – makes it an offence to unlawfully produce, sell, offer to sell, procure for use, design, adapt for use, distribute or possess any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section; and
- section 86(4) – makes it an offence to utilise any device or computer program mentioned in section 86(3) in order to unlawfully overcome security measures designed to protect such data from access thereto.

Under the ECT Act, the maximum penalty for contravening section 86(5) is a fine (unspecified) or imprisonment for a period not exceeding five years.

Phishing

Yes. Phishing is recognised as an offence under section 87(2) of the ECT Act, which provides that a person who commits any of the acts described in sections 86(1)–86(5) for the purpose of obtaining an unlawful advantage by causing fake data to be produced with an intent that it would be considered or acted upon as if it were authentic is guilty of offence. The maximum penalty under the ECT Act is a fine (unspecified) or imprisonment for a period not exceeding five years.

Phishing can also be prosecuted under the common law offences of theft and fraud. The maximum penalty imposed would depend on which court hears the case (which would depend on a variety of factors, the quantum of the claim being one). If the case is prosecuted in the Magistrate's Court, the court can impose a fine or imprisonment for a maximum period of 15 years in terms of its penal jurisdiction. If the case is heard in the High Court of South Africa, the court has wider discretion and may impose any fine or term of imprisonment which they deem appropriate in the circumstances.

Under the Cybercrimes Bill, there are separate offences for cyber fraud, cyber forgery and uttering and cyber extortion (sections 8, 9 and 10) which all attempt to deal with forms of phishing. A court which convicts a person of such an offence (where a penalty is not prescribed by any other law) can impose a sentence which the court deems appropriate and which is within that court's penal jurisdiction.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. See the discussion above in respect of denial-of-service attacks. Section 87(1) relating to computer-related extortion, fraud and forgery of the ECT Act is also relevant as it states that it is an offence to perform or threaten to perform any of the acts described in section 86, for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions.

Under the ECT Act, the maximum penalty imposed for contravention of section 86(4) or 87 is a fine (unspecified) or imprisonment for a period not exceeding five years.

Under the Cybercrimes Bill, there are separate offences for unlawful acts (in respect of software or hardware tools), as well as unlawful interference with data, a computer program, a computer data storage medium or a computer system (which is construed broadly enough to specifically include malware).

Under the Cybercrimes Bill, the maximum penalty for contravention of these sections is a fine (unspecified) or imprisonment for a period not exceeding 10 years (or both).

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Yes. See the discussion above in respect of denial-of-service attacks. Section 86(3) of the ECT Act is relevant and the maximum penalty which can be imposed for contravention of section 86(3) is a fine or imprisonment for a period not exceeding 12 months.

Under the Cybercrimes Bill, it is an offence under section 4(1) to unlawfully and intentionally possess, manufacture, assemble, obtain, sell, purchase, make available or advertise any software or hardware tool for purposes of contravening certain other section of the Cybercrimes Bill. The maximum penalty for contravention of this section is a fine (unspecified) or imprisonment for a period not exceeding 10 years (or both).

Identity theft or identity fraud (e.g. in connection with access devices)

Yes. Section 87 of the ECT Act (which deals with computer-related extortion, fraud and forgery) is relevant and criminalises the actions of a person who performs or threatens to perform any of the acts in section 86 for the purpose of obtaining any unlawful proprietary advantage, or obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic. If the offender uses an access device to breach certain security measures and then uses the data unlawfully, then the offender will have contravened section 87 and 86 of the ECT Act. As stated above, the maximum penalty imposed for contravention of section 87 is a fine (unspecified) or imprisonment for a period not exceeding five years.

Identity theft or fraud can also be prosecuted under the common law offence of "theft" or "fraud". The sentencing jurisdiction would operate the same as discussed above in relation to "phishing".

Depending on the nature of the offence, it may also be possible to prosecute identity theft or fraud as an infringement of copyright under copyright laws.

Under the Cybercrimes Bill, there are separate offences for cyber fraud, cyber forgery and uttering and cyber extortion (sections 8, 9 and 10) which are broad enough to cover identity theft or fraud. A court which convicts a person of such an offence (where a penalty is not prescribed by any other law) can impose a sentence which the court deems appropriate and which is within that court's penal jurisdiction.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Yes. Electronic theft may constitute an offence under section 86(1) of the ECT Act relating to unlawful access to data (see the discussion above in relation to hacking). It can also be prosecuted under the common law offence of theft.

Breach of confidence by a current/former employee would be actionable as a common law delict (tort), but not necessarily as a criminal offence.

With regards to criminal copyright infringement, the Copyright Act 98 of 1978 makes provision for criminal penalties, including a fine (a maximum of R5,000 per infringement) and/or imprisonment of up to three years for a first conviction. The maximum fine and/or imprisonment penalty for a second conviction is R10,000 and/or five years.

See also the discussion above in relation to hacking with regards to the Cybercrimes Bill and electronic theft.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The ECT Act also criminalises attempting to commit any of the offences in the ECT Act or aiding and abetting those offences (section 88). The same penalties would apply as if the offence was successfully perpetrated.

Under the Cybercrimes Bill there are numerous new offences relating to "malicious communications". For example, it will be an offence to disseminate a data message which advocates, promotes or incites hate, discrimination or violence against a person or group of persons. "Revenge porn" will also constitute an offence under the Cybercrimes Bill (where a naked image of a person is shared electronically without their consent). The infringement of copyright (through the use of peer-to-peer file sharing) is also an offence under the Cybercrimes Bill.

Failure by an organisation to implement cybersecurity measures

Under the current legislative framework, there is no law which imposes a duty to implement cybersecurity measures on an organisation.

However, the Protection of Personal Information Act 4 of 2013 ("**POPI Act**"), which was promulgated in 2013 but which has not yet commenced, does contain obligations for responsible parties (data controllers) to implement reasonable technical and organisational measures to safeguard personal information in their possession or control against unauthorised access, which will likely involve cybersecurity measures. The POPI Act further imposes administrative fines as well as punitive penalties for infringement of its provisions.

The Cybercrimes Bill imposes extensive cybersecurity obligations on electronic communications service providers, financial institutions, payment system institutions and any company, entity or person who is declared by the Minister of State Security to own or control a critical information structure. The Cybercrimes Bill establishes various cybersecurity structures such as the 24/7 point of contact, the Cybersecurity Hub and nodal points to promote the reporting, investigation and prosecution of Incidents of cybercrime.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Section 90 of the ECT Act lists the instances where South African courts will have extra-territorial jurisdiction in respect of cyber-related offences. This includes where the offence was committed in South Africa, where any preparatory act towards the offence was committed in South Africa, where the offence was committed by a citizen, resident or person carrying on business in South Africa or where the offence was committed on board any ship or aircraft registered in South Africa or on a voyage or flight to or from South Africa at the time the offence was committed.

Under the Cybercrimes Bill, the extraterritorial jurisdiction provisions are more extensive and even where an offence is committed outside of South Africa, a South African court will have jurisdiction if the person charged: is a citizen or ordinary resident of South Africa, was arrested in South Africa (or onboard a vessel registered in South Africa); or is a company or body of persons incorporated or registered in South Africa. An offence shall also be deemed to have been committed in South Africa under the Cybercrimes Bill if the act or commission affects or is intended to affect any person in South Africa or the perpetrator is found to be in South Africa; or if the perpetrator is not extradited by South Africa.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

There are no provisions in the ECT Act which deal with exceptions or mitigation of sentences. This would need to be considered by a court on a case-by-case basis.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Certain terrorism offences may arise in relation to cybersecurity or an Incident. South Africa does have in place legislation criminalising acts of terrorism, but it is broad enough to cover a multitude of scenarios. The offence of treason is a common law offence and defined as "any conduct unlawfully committed by a person owing allegiance to a state with the intention of: (i) overthrowing the government of the Republic; (ii) coercing the government by violence into any action or inaction; (iii) violating, threatening or endangering the existence, independence or security of the Republic; and (iv) changing the constitutional structure of the Republic". The offence of treason may therefore also be construed broadly enough to include an Incident. We are not aware of any specific prosecutions in the cybersecurity context.

Under the Cybercrimes Bill, there is a new offence which relates to computer-related terrorist activity as the propagation of terrorist activities to recruit new members, disseminating information on how to make bombs or weapons, online co-ordination of terrorist attacks and any activity aimed at causing destruction, destabilisation or threatening national or international security.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The legislative frameworks in South Africa that are relevant to cybersecurity are set out below:

- The right to privacy is enshrined in section 14 of the Constitution of South Africa, 1996 and states that "everyone has the right to privacy, which includes the right not to have their privacy of their communications infringed".
- In order to give effect to the right to privacy, the POPI Act was promulgated. The POPI Act is data protection legislation primarily modelled on the EU general data protection laws. Importantly, it establishes the Information Regulator and confers various powers, duties and functions including monitoring and enforcing compliance by public and private bodies and handling complaints in respect of contraventions of the POPI Act. It also establishes a comprehensive compliance framework and places cybersecurity obligations on responsible parties to secure the integrity and confidentiality of personal information in its possession or control by taking appropriate, reasonable technical and organisational measures to prevent unlawful access. The substantive provisions of the POPI Act are not yet in effect. The commencement date of the POPI Act is imminent.
- The ECT Act, as discussed in section 1 above, regulates electronic communications and transactions and is the primary legislation currently in force which criminalises cyber-related offences.
- The Cybercrimes Bill, as discussed in section 1 above, which is not yet in force, aims to consolidate and put in place a comprehensive cybersecurity framework and provides for the criminalisation of a broad range of cyber-related crimes.
- The Regulation of Interception of Communications and Provision of Communications-related Information Act 70 of 2002 ("**RICA**") regulates the interception and monitoring of direct and indirect communications. RICA contains exceptions relating to where interception and monitoring takes place with the consent of the parties involved or where it is carried out by law enforcement personnel.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

There is no legislation in force which specifically relates to cybersecurity requirements applicable to critical infrastructure at present.

However, the Cybercrimes Bill (sections 58–60) will put in place measures to designate national critical information infrastructures and the mechanisms established to deal exclusively with the protection of such critical infrastructure. Information infrastructures will be declared as national critical information infrastructures if it appears that the information is of such a strategic nature that the interference, damage or loss thereof may prejudice state security, public health, the

rendering of essential services, economic stability or create a public emergency. There are procedures which the Minister of Security must follow before information infrastructures can be declared critical.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Once the POPI Act comes into operation, the responsible party (similar to data controller) will be required to take appropriate reasonable technical and organisational measures to prevent unlawful access to personal information in its possession or control (section 19). This obligation will include taking measures to monitor, detect, prevent or mitigate Incidents. As the POPI Act is not yet in effect, the Information Regulator has not published any regulations or guidance on what measures are required to be taken.

The King IV Report on Corporate Governance for South Africa – 2016 ("**King IV**") is a set of voluntary principles in the area of corporate governance. Companies listed on the Johannesburg Stock Exchange are, however, required to comply with King IV by law. In particular, King IV has a specific focus on the oversight of information and technology management. The board of the company is specifically tasked to make sure it proactively monitors cyber Incidents and ensure that it has systems and processes in place from a cybersecurity perspective.

The Cybercrimes Bill also places obligations on electronic communication service providers (which includes financial institutions and any entity or person who is declared by the Minister of State Security to own or control a critical information structure) which become aware that its electronic communications network is being used to commit an offence to immediately report the matter in the prescribed manner to the South African Police Services and preserve all information/evidence that will be relevant to the investigation of the offence.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Not at this stage, as the provisions of the POPI Act are not yet in force. The Cybercrimes Bill has also not been promulgated into law yet.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Under current law, there is no duty to report Incidents to a regulatory or other authority.

Once the POPI Act comes into operation, section 22 provides that responsible parties must inform both the Information Regulator and the affected data subjects (unless the identity of such data subjects cannot be established) in writing as soon as reasonably possible that there is a breach or suspected breach – where there are reasonable grounds to believe that personal information of a data subject has been accessed or acquired by an unauthorised person. The notification must contain sufficient information to enable the data subject to take protective measures against potential consequences of the Incident. The Information Regulator may also direct the responsible party to publicise such Incident.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

There is no prohibition under current laws which would prevent organisations from voluntarily sharing information relating to Incidents with regulatory authorities in South Africa or outside of South Africa, provided such information is not subject to confidentiality restrictions, deemed classified or otherwise restricted.

The POPI Act is, however, not yet in operation, so the Information Regulator has not published any regulations or guidance notes on this issue.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes, see the answer to question 2.5 above.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

At this stage, the reporting and notification obligation under the POPI Act will only apply to the extent that the Incident involves personal information. IP addresses and email addresses may constitute personal information. Once the POPI Act comes into operation, the Information Regulator may also publish regulations or exemptions on this issue.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Under the POPI Act, the Information Regulator (http://www.justice.gov.za/inforeg/) is responsible for enforcing the requirements.

Under the Cybercrimes Bill, the following authorities are relevant:

- the South African Police Services;
- the State Security Agency; and
- the National Prosecuting Authority.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The Information Regulator may impose administrative fines on responsible parties to a maximum of R10 million. Depending on the offence, the POPI Act also provides for fines and imprisonment not exceeding 10 years.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The POPI Act and Cybercrimes Bill are not yet in force and accordingly no enforcement action has been taken. Once the POPI Act comes into force, there will be a grace period of one year (which may be extended for up to three years) for responsible parties to comply with the provisions of the POPI Act.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

While there are no strict legal requirements under Applicable Laws which require different business sectors to address cybersecurity differently, certain sectors such as financial services (in particular banks and insurers who hold licences) tend to be more incentivised to avoid the cost and reputational impact of Incidents. As the POPI Act has been promulgated (but not yet effective) for a few years now, many organisations' cybersecurity practice is driven not just by "compliance" but also promoting good business practices. Once the POPI Act comes into force, the Information Regulator may publish industry-specific Codes of Conduct for different business sectors.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

No, not at present.

However, the Cybercrimes Bill will place obligations on electronic communication service providers (which includes financial institutions and any entity or person who is declared by the Minister of State Security to own or control a critical information structure) which become aware that its electronic communications network is being used to commit an offence to immediately report the matter in the prescribed manner to the South African Police Services and preserve all information/evidence that will be relevant to the investigation of the offence.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

See the discussion above under question 2.3 relating to King IV, which places obligations on the board of directors of the company to make sure it proactively monitors cyber Incidents and ensure that it has systems and processes in place from a cybersecurity perspective.

While the principles in King IV are voluntary (except for listed companies), failure by a company to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties both under the common law and the Companies Act 71 of 2008 ("**Companies Act**").

Under the common law, a breach of fiduciary duties may apply, and the director can be held liable for any losses, damages or costs. Section 76 of the Companies Act sets out standards of directors conduct and that a director must always act in good faith, for a proper purpose, in the best interest of the company and with a degree of reasonable care, skill and diligence. Failure to prevent, mitigate, manage or respond to an Incident may amount to a breach of directors' duties under the Companies Act.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

No, there are no Applicable Laws which require companies to satisfy any of the specific requirements above. However, see the discussion above under question 2.3 relating to King IV, which places obligations on the board of directors of the company to make sure it proactively monitors cyber Incidents and ensures that it has systems and processes in place from a cybersecurity perspective.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no additional requirements other than what has been set out under questions 2.5 and 2.7 above.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, there are no other specific requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

There are a variety of civil actions which may be brought in relation to an Incident; the most relevant would probably be a claim for compensation (or damages) under a delictual action (*action lex aquila* – similar to tort). The claimant would need to claim against the organisation or individual which caused the Incident. In order to be entitled to compensation in damages, the claimant would need to prove: (i) a wrongful act or omission (i.e. the Incident); (ii) caused by negligence/fault/breach of duty of care; and (iii) actual monetary loss on the part of the claimant.

It is also conceivable that an Incident would, depending on the circumstances, give rise to a claim for breach of contract where the particular Incident constituted a breach of contract between the parties.

Section 99 of the POPI Act also provides for civil remedies in terms of which a data subject or the Information Regulator may institute a civil action for damages against a responsible party for breach of the provisions of the POPI Act (as referred to in section 73) whether or not there is intent or negligence on the part of the responsible party.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

As far as we are aware, there have not been any specific cases in relation to Incidents brought in South Africa.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes; see the answer to question 5.1 above.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, although this is still relatively new in South Africa and the market has been slow to take up cyber-risk insurance cover (because South Africa has been slow in promulgating its data protection and cybersecurity legislation). Typically, this sort of insurance would cover business interruption, system failures, cyber extortion, etc.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limits on what the insurance policy can cover. The general rules of insurance would apply.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

No, there is no legislation which requires the monitoring of employees for the purposes of preventing, detecting, mitigating and responding to Incidents. Monitoring of employees' use of email and internet access, for example, will involve the processing of personal information and therefore the POPI Act (once effective) will apply.

RICA regulates the interception and monitoring of direct and indirect communications. RICA contains exceptions relating to where interception and monitoring takes place with the consent of the parties involved or where it is carried out by law enforcement personnel.

While there are no specific laws which place a duty on employees to report cyber risks, security flaws, Incidents or potential Incidents to their employers, once the POPI Act comes into effect it is likely that the employee (in the capacity of an operator) will have to notify the responsible party immediately if there are reasonable grounds to believe that the personal information of a data subject has been accessed by an unauthorised person.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no Applicable Laws which may prevent or limit the reporting of Incidents by an employee. For whistle-blowers, the employee would need to satisfy the whistleblowing provisions in the Protected Disclosures Act 26 of 2000, one of which is that the subject matter of the disclosure falls into one or more categories. The categories include criminal offences and breach of a legal obligation, which may be appropriate for Incidents, although may not be wide enough to cover security flaws or mere risks.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Currently, the South African Police Services has general law enforcement and investigatory powers to investigate an Incident. The Criminal Procedure Act 51 of 1977 sets out the procedure to be followed by the South African Police Services when investigating a criminal offence.

The POPI Act grants broad powers to the Information Regulator to, *inter alia*, commence an investigation at their own initiative, summon people to appear before it and give evidence, enter and search any premises, conduct interviews, carry out enquiries as the Information regulator sees fit and refer complaints to other bodies.

The Cybercrimes Bill establishes procedures which specifically cater for the investigation of cyber-related offences. The Cybercrimes Bill confers extensive powers to law enforcement authorities and other investigators in respect of access, search and seizure of articles involved in the commission of an offence. It also establishes a 24/7 point of contact and mutual legal assistance in the arena of cybercrimes (different law enforcement agencies working together to facilitate enforcement and compliance). The Cybercrimes Bill also authorises the President of South Africa to enter into agreements with foreign states for the provision of mutual assistance and co-operation relating to the investigation and prosecution of cyber-related offences.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no such requirements under the Applicable Laws.

Fatima Ameer-Mia
Cliffe Dekker Hofmeyr Inc
11 Buitengracht Street
Cape Town, 8001
South Africa

Tel: +27 21 481 6374
Email: fatima.ameermia@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

Fatima Ameer-Mia is a senior associate in the Technology & Sourcing practice. Fatima specialises in commercial contracts, information technology, intellectual property and data protection law. She also has a special interest in the fields of e-commerce, information security and matters relating to cybercrime.

Fatima advises clients, both locally and internationally, in various sectors on their commercial and technology arrangements, including outsourcing, software licensing and development and systems integration.

She regularly advises on data protection and information security, including providing training, seminars, risk assessments and governance frameworks on cybersecurity and data protection laws.

Christoff Pienaar
Cliffe Dekker Hofmeyr Inc
11 Buitengracht Street
Cape Town, 8001
South Africa

Tel: +27 21 481 6350
Email: christoff.pienaar@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

Christoff Pienaar is Director and National Head of the Technology & Sourcing practice at Cliffe Dekker Hofmeyr Inc and is admitted to practise as an attorney of the High Court of South Africa and as a solicitor of the Senior Courts of England and Wales. He advises on commercial, information technology and intellectual property law. He specialises in information technology and commercial matters and has particular expertise in payment systems, technology outsourcing, business process outsourcing, data protection, information security, systems integration, hardware acquisitions and maintenance, IT consultancy services, managed services, disaster recovery services, software development and software licensing and support transactions. Christoff also advises on general commercial and intellectual property issues across a diverse range of industry sectors, especially financial services.

CDH
CLIFFE DEKKER HOFMEYR

Cliffe Dekker Hofmeyr Inc is one of the largest business law firms in South Africa, with more than 350 lawyers and a track record spanning over 164 years. The Technology & Sourcing practice of Cliffe Dekker Hofmeyr Inc is widely recognised as a market leader for its work with a large proportion of the top financial institutions in South Africa on their headline technology projects. The team is renowned across the technology and telecoms industries for its market-leading position in all of information technology, telecoms and privacy & data protection. The team handles domestic and global mandates and is involved in changes to key legislation affecting these sectors.

Sweden

Anders Hellström

Erik Myrberg

Synch

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes, according to the Swedish Penal Code, hacking (intentionally giving oneself unauthorised access to electronic information) is considered a data breach (Sw. *Dataintrång*). The penalty for data breach is either a fine or a maximum of two years in prison. Serious offences of data breach are punishable with at least six months in prison but no more than six years.

The Swedish Supreme Court found a police officer guilty of a data breach and sentenced the police officer to a fine. The police officer used the Swedish police's internal IT system to search for himself with the purpose of finding out whether any information was registered about him or not. The police officer had proper access to the systems for other purposes, but no authorisation to carry out such a search.

Denial-of-service attacks

Yes, according to the Swedish Penal Code, denial-of-service attacks (intentionally causing a severe disturbance or hindering access to electronic information) is considered a data breach. The penalty for data breach is either a fine or a maximum of two years in prison. Serious data breach offences are punishable with at least six months in prison but no more than six years.

The Swedish Court of Appeal sentenced a man to imprisonment for shutting down the websites of two major banks in Sweden for a duration of 45 minutes by using denial-of-service attacks. Due to the offender's age, the imprisonment was changed to a conditional sentence.

Phishing

Phishing is covered by the provision on fraud in the Swedish Penal Code. The penalty for the crime is either a fine or a maximum of two years in prison. Serious offences of fraud are punishable with at least six months in prison but no more than six years.

The District Court of Malmö sentenced four persons to imprisonment for sending emails imitating email communication from banks. The emails caused some recipients to provide their payment information to the fraudsters in the belief that they communicated with the bank.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

The Swedish Court of Appeal has ruled that the installation of a program on an IT system without permission is not a crime in itself. If the installation is harming or disturbing electronic information on the computer on which it is installed, the prerequisites for data breach are met according to the Swedish Penal Code. The penalty for data breach is either a fine or a maximum of two years in prison. Serious offences of data breach are punishable with at least six months in prison but no more than six years.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

The mere possession of hacking tools is not criminalised in Sweden but preparation for a data breach is considered a crime according to the Swedish Penal Code. The penalty for the crime is a fine or a maximum of two years in prison. A preparation for a serious data breach offence is punishable with at least six months in prison but no more than six years.

The Swedish Copyright Act prohibits the use, development, marketing and possession of technical instruments, components and services whose purpose is to gain unauthorised access to material protected by copyright.

Furthermore, the Swedish Act on Decoding prohibits the use, development, marketing and possession of hardware and software which is designed to be used for decoding the services defined in the abovementioned law (e.g. radio and TV broadcasting to the public).

Identity theft or identity fraud (e.g. in connection with access devices)

Yes, identity theft and identity fraud are crimes according to the Swedish Penal Code. The penalty for the crime is either a fine or a maximum of two years' imprisonment.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Copyright infringement is regulated by the Swedish Copyright Act. The penalty for copyright infringement is either a fine or a maximum of two years in prison. The Swedish Supreme Court sentenced a man to imprisonment (which was later changed to a fine) for making available 125 movies and TV series to the public without the rightsholders' permission. The movies and TV series were shared online through torrent files.

It is not a criminal offence if a current or former employee is disclosing information subject to confidentiality which is imposed on the employee by a contract between him/her and the employer. Certain categories of work are subject to statutory confidentiality (e.g. lawyers and doctors). For example, a lawyer is not allowed to

disclose information regarding his clients according to the Swedish Code of Judicial Procedure (Sw. *Rättegångsbalken*). According to the Swedish Penal Code, disclosure of information subject to statutory confidentiality is punishable with a fine or a maximum of one year in prison.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Further to what is mentioned above, it can be noted that destroying or causing damage to physical equipment such as computers, servers and transmitters would in general be considered acts of damage to property (Sw. *skadegörelse*), which is criminalised under the Swedish Penal Code and sanctioned by up to two years' imprisonment.

Where such equipment is of importance to national security, the legal system, public order or administration, the destruction or damaging thereof may be considered to be sabotage according to the Swedish Penal Code. The penalty for sabotage is either a fine or a maximum of two years in prison. Serious offences are punishable with at least six months in prison but no longer than six years.

Failure by an organisation to implement cybersecurity measures

Applicable data protection and telecoms law contains provisions addressing the failure to implement security measures regarding processing of personal data and keeping IT systems secured. Such failure is usually punished by a regulatory fine.

In the context of criminal law, the Swedish Penal Code does not criminalise the failure by an organisation to implement cybersecurity measures.

1.2 Do any of the above-mentioned offences have extraterritorial application?

First, it shall be noted that double criminality applies in Sweden. In order for a crime committed abroad to be punishable in Sweden, it also needs to be criminalised in the country where it is perpetrated (with some exceptions). Consequently, according to the Swedish Penal Code, extraterritorial application regarding data breach applies if the offence is carried out by a Swedish citizen or a foreigner living in Sweden and the act is also criminalised in the country where it is carried out. Swedish law also applies if a crime that can be punishable with more than six months in prison has been carried out abroad by a foreigner who does not live in Sweden, but is located in the country.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

According to the Swedish Penal Code, a penalty can be mitigated if the offender can prove that he/she tried to reduce or hinder the offence.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Hacking can be considered a terrorism offence if the act has the potential to cause severe damage to a country or an IGO and the intention of the act is to (i) create serious fear amongst a group of people, (ii) force a government or an IGO to act in a way preferred to the party carrying out the hacking, or (iii) cause serious destabilisation or destroy constitutional, political, economical or social structures of a state or an IGO. The penalty for the crime is a minimum of two years in prison with the maximum of a life sentence.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

- The processing of personal data is regulated by the EU General Data Protection Regulation (GDPR).
- The processing of personal data by governmental agencies regarding prevention, investigation, prosecution and the like is regulated by the Swedish Act on Processing of Personal Data Relating to Criminal Offences (Sw. *Brottsdatalagen*).
- Criminal offences (e.g. hacking, denial-of-service attacks, phishing, etc.) is subject to the Swedish Penal Code (Sw. *Brottsbalken*).
- Copyright infringement is governed by the Swedish Copyright Act (Sw. *Lag om upphovsrätt till litterära och konstnärliga verk*).
- Decoding of radio and TV is regulated by the Swedish Act on Decoding (Sw. *Avkodningslagen*).
- Terrorism offences in the context of cybersecurity are regulated by the Swedish Act on Criminal Responsibility for Terrorist Offences (Sw. *Lag om straff för terroristbrott*).
- The Swedish Act on Electronic Communication regulates the providers of electronic communications (Sw. *Lag om elektronisk kommunikation*).
- The Directive on Security of Network and Information Systems (NIS) is implemented in Sweden as the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services and regulates providers of services critical for infrastructure and the security of their IT systems (Sw. *Lag om informationssäkerhet för samhällsviktiga och digitala tjänster*).
- The Swedish Act on Payment Services (Sw. *Lag om betaltjänster*).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The requirements under the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services are not in excess of the requirements of the NIS Directive.

The abovementioned act applies to legal entities who provide services critical for infrastructure (e.g. banks and health services). The purpose of the legislation is to harmonise and improve the security of the providers of essential services and their IT systems throughout the EU.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The GDPR puts obligations on data controllers to implement appropriate technical and organisational measures when processing personal data. Not all of these measures are explicitly defined but include requirements to monitor, detect, prevent and mitigate Incidents.

The Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services requires providers of services critical for infrastructure to implement appropriate and proportionate technical and organisational measures regarding their IT systems. Not all of these measures are explicitly defined but include requirements to monitor, detect, prevent and mitigate Incidents.

The Swedish Act on Electronic Communication put obligations on electronic service providers to implement appropriate technical and organisational measures regarding the services they provide. Not all of these measures are explicitly defined but include requirements to monitor, detect, prevent and mitigate Incidents.

The Swedish Act on Payment Services ensures that providers of payment services must implement technical and organisational measures to ensure the safety of money transactions. As with previously mentioned laws, no explicit definitions of the measures are present but include requirements to monitor, detect, prevent and mitigate Incidents.

Governmental authorities shall follow the regulations drafted by the Swedish Civil Contingencies Agency. The regulations include, for example, drafting security policies and documenting security actions taken.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

To date, no issues regarding conflict of laws have been brought to attention. The GDPR and the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services may apply at the same time but regulate different aspects. Electronic service providers subject to the Swedish Act on Electronic Communication have been explicitly excluded from the scope of the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services.

Criminal offences regarding data breaches are subject to the Swedish Penal Code, which does not interfere with applicable data protection law.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Data controllers subject to the GDPR are obligated to notify the Swedish Data Protection Authority without undue delay when becoming aware of a personal data Incident that is not considered to be of minor importance. The notification must include a description of the nature of the Incident (e.g. number of affected individuals and categories of data subjects). The data controller also needs to communicate its contact details, likely consequences of the personal data breach and describe measures taken/proposed to be taken to address the data breach (including appropriate measures to mitigate possible adverse effects).

The Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services requires providers of services critical for infrastructure (e.g. banks and health services) to report Incidents to the Swedish Civil Contingencies Agency without undue delay. Provisions explicitly defining what information an Incident report shall include are to be set out in the regulations set by the supervisory authority.

The Swedish Act on Electronic Communication puts obligations on electronic service providers to notify severe interruptions to the Swedish Post- and Telecom Authority without undue delay. The provider shall notify the Swedish Post- and Telecom Authority within 24 hours of an integrity Incident being discovered. An Incident is defined as an unlawful destruction, loss or change of, or unlawful disclosure or access to, information. The provider must also notify affected subscribers with information (for example, when the Incident occurred, recommended measures, contact details).

The Swedish Act on Payment Services obligates providers of payments services to report Incidents in their operations to the Swedish Financial Supervisory Authority. The notifications shall be sent without undue delay. The providers shall also notify affected individuals. The notification must include information about the Incident and how to mitigate the damage.

As a general rule, the Principle of Public Access to Official Records (Sw. *Offentlighetsprincipen*) gives individuals the right to request and access documents received by a governmental agency. Upon such request, the Swedish Data Protection Authority carries out a test whether the Incident report is subject to confidentiality or not. To date, the Swedish Data Protection Authority has not granted any requests regarding making an Incident report public.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Organisations are permitted to voluntarily share information with regulatory and/or other authorities and organisations, subject to

compliance with any secrecy restrictions which may apply under law. If the information includes personal data, the GDPR applies.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

According to the GDPR, data controllers shall communicate the personal data breach to the data subject without undue delay if the personal data breach is likely to result in a high risk to the rights and freedoms of the affected natural persons.

Subscribers to electronic services affected by an Incident have the right to be informed by the service provider without undue delay according to the Swedish Act on Electronic Communications.

The Swedish Act on Payment Services puts obligations on providers of payment services to report Incidents to the users of the payment services if there is a risk that their transactions may be affected.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Any information relating to an identified or identifiable person constitutes personal data which needs to be processed in accordance with the GDPR. Therefore, a data controller is not permitted to communicate information regarding a data breach without, e.g., a legal ground and purpose.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The GDPR authorises the Swedish Data Protection Authority to monitor and enforce the application of the GDPR. This includes many different tasks such as conducting investigations, promoting public awareness, handling complaints and giving advice.

The Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services stipulates that the Swedish Civil Contingencies Agency shall carry out supervision to ensure that providers of services critical for infrastructure (e.g. banks and health services) abide by the security measures that the law prescribes.

The Swedish Act on Electronic Communication states that the Swedish Post- and Telecom Authority is responsible for monitoring electronic service providers' compliance with the law.

The Swedish Act on Payment Services authorises the Swedish Financial Supervisory Authority to carry out supervision regarding providers of payments services.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The GDPR prescribes that a failure to report an Incident involving personal data and/or to implement appropriate technical and organisational measures can result in a fine. The fine varies depending on the infringement and can under certain circumstances amount to either 10,000,000 euros or 2% of the data controller's total worldwide annual turnover of the preceding financial year, whichever is higher.

The Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services prescribes that failure to comply with the law will result in a fine starting at a minimum of 5,000 SEK up to a maximum of 10,000,000 SEK.

Not complying with the Swedish Act on Electronic Communication can result in a fine or a maximum of six months in jail. Legal entities violating the law shall pay damages to the injured party.

A violation of the Swedish Act on Payment Services can result in a fine starting at a minimum of 5,000 SEK up to a maximum of 50,000,000 SEK.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The Swedish Data Protection Authority initiated its first investigations in June 2018 to verify compliance with the GDPR among companies in Sweden and has not reported any findings yet.

However, companies have been subject to measures before the entry into force of the GDPR. The Swedish Data Protection Authority forced a large debt collection company to introduce more mechanisms to ensure a higher level of safety for the personal data processed by the company. The company appealed against the decision but lost.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Companies and organisations can implement standards such as ISO 27002:2013 and NIST 800-88 to ease the process of regulatory compliance. These standards are not mandatory, and it is hard to draw any general conclusion about which business sectors are more likely to implement such standards. The financial and telecom sectors are more regulated than other business areas.

The Swedish Standards Institute (SSI) is a part of the European Committee for Standardization. SSI provides standards to its members and always adopts the European standard. Currently 1,300 companies, agencies and organisations are members.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The Swedish Financial Supervisory Authority drafts regulations and guidelines regarding the financial sector. According to the regulations, the affected companies shall have a structure and management for IT security involving, for example, physical security measures, reporting systems and control of access to information.

The GDPR put obligations on data controllers to implement appropriate technical and organisational measures when processing personal data. Not all of these measures are explicitly defined but include requirements to monitor, detect, prevent and mitigate Incidents.

The Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services requires providers of services critical for infrastructure to implement appropriate and proportionate technical and organisational measures regarding the systems they use. Not all of these measures are explicitly defined but include requirements to monitor, detect, prevent and mitigate Incidents.

The Swedish Act on Electronic Communication puts obligations on service providers to implement appropriate technical and organisational measures regarding the services they provide. Not all of these measures are explicitly defined but include requirements to monitor, detect, prevent and mitigate Incidents.

The Swedish Act on Payment Services ensures that providers of payment services must implement technical and organisational measures to ensure the safety of money transactions. As with the previously mentioned laws, no explicit definitions of the measures are present but include requirements to monitor, detect, prevent and mitigate Incidents.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

There are no such obligations for directors. Anyone who is in breach of the laws mentioned in question 3.2 can be held responsible and charged with a fine. Violations of the Swedish Act on Electronic Communication can result in imprisonment if the breach is carried out by an individual.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The GDPR, the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services and the Swedish Act on Electronic Communications all require but do not define technical and organisational measures.

The technical measures required would likely be assessed based on market standard and best practice, and might include that service providers of critical infrastructure have to carry out penetration tests in order to be compliant with the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services. It is also possible that organisational measures include that a data controller must establish a written Incident response plan in order to be compliant with the GDPR.

However, no applicable law explicitly places obligations on private or listed companies to, e.g., designate a CISO.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Listed companies are required to disclose any information (regardless of whether it derives from a cybersecurity breach or not) that may affect the price of the company shares according to the Swedish Act on Markets for Financial Instruments (Sw. *Lag om värdepappersmarknaden*) and soft law (Sw. *Regelverk för emittenter NASDAQ Stockholm*).

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

There are no explicit obligations under law placed upon private or listed companies regarding cybersecurity in Sweden.

Listed companies are subject to soft law (Sw. *Svensk kod för bolagsstyrning*), which states that the board of directors in a listed company should have the competence to manage the company with integrity and efficacy. Therefore, one can expect a listed company to implement satisfactory measures for ensuring a reasonable level of IT security.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

A person or a company is able to seek monetary remedies in court for data breaches occurring from a contractual relationship. Such breaches and the consequences thereof are often regulated in the agreement between the parties.

Data subjects may file a lawsuit against a data controller for processing personal data without legal grounds, transferring personal data to a third party without prior permission, or not assisting the data subject to exercise its data subject rights according to the GDPR. Such violations can result in damages to the data subject. The data subjects are also able to claim for a declaratory judgment regarding its own rights (e.g. the right to be forgotten).

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Private litigation regarding cybersecurity is uncommon in Sweden. In 2013, a plaintiff was awarded damages of 3,000 SEK by the Supreme Court in a civil case regarding the publication of a judgment on a public website. The publication was found to violate the plaintiff's personal integrity according to current data protection legislation.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

The Swedish Tort Liability Act (Sw. *Skadeståndslagen*) is subsidiary to other laws and hence where the GDPR regulates the data subjects' right to monetary damages, this will apply instead. The act is also dispositive in a contractual context, i.e. parties to a contract are free to regulate the consequences of an Incident differently between themselves.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

It is possible to take out insurance against claims from third parties due to a data breach. Fines imposed by regulatory authorities might

be possible to insure against, but the legal situation is not clear. The nature of the fine (e.g. punitive or not) and the conduct (e.g. mere negligence, gross negligence or intent) are factors that need to be considered.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No. However, it is unclear whether it is possible to insure yourself against regulatory fines or not.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

If the monitoring of the employees constitutes processing of personal data, the GDPR applies. The relationship between an employee and an employer is considered to have an inherent imbalance of power and therefore an employee is normally considered not to be able to freely consent to monitoring. Instead, the employer will need to ensure that such supervision is based on an alternative legal ground.

Due to the duty of loyalty arising from the employment contract, an employee may have to report Incidents to the employer.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

The Swedish Act on Whistleblowing (Sw. *Lag om särskilt skydd mot repressalier för arbetstagare som slår larm om allvarliga missförhållanden*) offers protection to employees disclosing information on severe misconduct in the workplace or in the employer's business. Severe misconduct aims at acts which would be punishable with imprisonment or equivalent offences. If the information is obtained through a criminal offence according to the Swedish Penal Code (e.g. hacking), the employee is not protected against reprisals.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

If the Incident is a criminal offence according to the Swedish Penal Code (or constitutes imprisonment), the Swedish Police and the Swedish Security Service have the authorisation to investigate. The latter is more usual regarding terrorism offences.

Incidents regarding personal data are subject to the Swedish Data Protection Authority. If the Incident is affecting the IT systems of providers of critical infrastructure, the Swedish Civil Contingencies Agency is the investigating power.

The Swedish Post- and Telecom Authority is responsible for investigating service providers who fail to report Incidents.

The Swedish Financial Supervisory Authority is authorised to investigate crimes regarding the Swedish Act on Payment Services.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Providers of electronic communication services are obligated upon request from law enforcement authorities to provide personal data if there is a suspicion of serious crime. The ECJ ruled in the Joined Cases C-203/15 and C-698/15 that such a request for disclosure shall be subject to preliminary review by a court or an independent administrative authority.

Anders Hellström
Synch
P.O. Box 3631
SE-103 59 Stockholm
Sweden

Tel: *+46 761 761 990*
Email: *anders.hellstrom@synchlaw.se*
URL: *www.synchlaw.se*

Anders Hellström has more than 12 years of experience as a commercial lawyer, starting out at Bird & Bird in 2006 and moving to Synch when it was founded in 2014. Prior to that, he served as an assistant judge at the District Court of Östersund during 2003–2005. During his career he has also been seconded to two major IT service providers for a total time of almost one year. Anders' focus area is commercial law, mainly working with companies in the IT and technology services sectors. He regularly provides advice to clients in commercial cases, assisting in a wide range of different matters and contracts, including licence agreements, outsourcing deals, service agreements and negotiations.

Erik Myrberg
Synch
P.O. Box 3631
SE-103 59 Stockholm
Sweden

Tel: *+46 761 761 948*
Email: *erik.myrberg@synchlaw.se*
URL: *www.synchlaw.se*

Erik Myrberg joined Synch in 2018 and works as a junior lawyer contributing to the commercial and data privacy practice of the firm. Erik acquired his Master of Laws degree from Uppsala University in 2018, focusing his Master's studies in the GDPR. He also studied courses in IT law, business law and EU law at Wirtschaftsuniversität Wien.

Synch is a business-oriented law firm with innovation and technology at its heart. We believe that lawyers and legal services always need to be in synch with the business environment. Legal services are to be provided in a pragmatic and accessible way. This is equally true for large, established industry companies as it is for small, fast-growing start-ups.

Synch wants to simplify the management of legal matters, both by providing packaged solutions and by making the best use of technology. In this way, Synch is able, and desires, to work more closely with its customers than traditional law firms, almost like an insourced legal department, taking part in the customers' daily business. Several of our lawyers are highly regarded individuals within their area of specialties and this has been recognised by the leading ranking institutes of legal services. Today Synch has offices in Stockholm, Copenhagen, Oslo and Silicon Valley.

Switzerland

Dr. András Gurovits

Niederer Kraft Frey Ltd.

Clara-Ann Gordon

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Hacking can constitute a criminal offence in Switzerland. Pursuant to Article 143bis of the Swiss Criminal Code (SCC), any person who obtains unauthorised access by means of data transmission equipment to a data processing system that has been specially secured to prevent such access is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty. If the hacker for his own or for another's unlawful gain obtains specially secured data which is not intended for him, he is liable, according to Article 143 SCC, to a custodial sentence not exceeding five years or to a monetary penalty.

In its decisions BGer 6B_615/2014 and 6B_456/2007, the Swiss Federal Supreme Court held that unauthorised access to another person's password-protected email account falls under the scope of the "hacking offence". In 2016, several hackers and persons threatening to hack IT systems of banks, universities and private enterprises could have been identified and arrested in Switzerland or abroad with the help of mutual legal assistance from foreign authorities.

Denial-of-service attacks

Denial-of-service attacks can constitute a criminal offence in Switzerland. Pursuant to Article 144bis SCC, any person who without authorisation alters, deletes or renders unusable data that is stored or transmitted electronically is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty. Moreover, data can also be regarded as rendered unusable if such data still exists but is temporarily inaccessible for authorised users, e.g. due to a denial-of-service attack.

Moreover, depending on the *modus operandi* of the individual case, the following further criminal provisions can be applicable in the context of denial-of-service attacks:

- extortion (Article 156 SCC) – penalty: a custodial sentence not exceeding five years; or a monetary penalty;
- coercion (Article 181 SCC) – penalty: a custodial sentence of up to three years; or a monetary penalty;
- misuse of a telecommunications installation (Article 179^{septies} SCC) – penalty: a fine upon complaint; and
- obstructing, disrupting or endangering the operation of a telecommunication service or utility provider (Article 239 SCC) – penalty: a custodial sentence of up to three years; or a monetary penalty.

Phishing

Depending on the individual design and purpose of a phishing mail or website, such phishing can constitute the following criminal offences:

- fraudulent use of a trademark or a copyright-protected work (Article 62 of the Swiss Trade Mark Protection Act, Article 67 of the Swiss Copyright Act);
- forgery of a document (Article 251 SCC); or
- computer fraud: unauthorised use of data and the transferring of financial assets through phishing (Article 147 SCC),

each of which is punishable by a custodial sentence not exceeding five years, or by a monetary penalty if committed for commercial gain.

Furthermore, in phishing cases, the criminal offence of money laundering (Article 305bis SCC), with a penalty of a custodial sentence not exceeding three years or a monetary penalty, can be part of the accusation (see the decision by the Swiss Federal Criminal Court, BG.2011.43).

The Office of the Attorney General of Switzerland has reported that, from 2012 to 2016, 455 criminal complaints with regard to phishing were filed by banks, authorities and private persons. Many cases were closed without an outcome due to lack of evidence or offenders remaining unidentified. Other cases, especially those involving requests for mutual legal assistance of foreign authorities, are still pending.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Such infections can be covered by Article 144bis SCC, prescribing that whoever alters, deletes or renders unusable data that is stored or transmitted electronically is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty ("virus offence").

Especially in connection with ransomware attacks, the following further criminal provisions can be applicable:

- fraud for commercial gain (Article 146 SCC) – penalty: a custodial sentence not exceeding 10 years; or a monetary penalty of not less than 90 daily penalty units;
- extortion (Article 156 SCC) – penalty: a custodial sentence not exceeding five years; or a monetary penalty; and
- money laundering (Article 305bis SCC) – penalty: a custodial sentence not exceeding three years; or a monetary penalty.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

While the mere possession of hacking tools is not illegal, the provision or use of hacking tools can constitute a criminal offence. According to Article 144bis paragraph 2 SCC, whoever manufactures, imports, markets, advertises, offers or otherwise makes accessible programs that will be used to alter, delete or render unusable data without authorisation is liable to a custodial sentence of up to three years or to a monetary penalty. In its decision BGE 129 IV 230, the Swiss Federal Supreme Court held that instructions and manuals explaining how to create programs that infect, destroy or render data unusable fall under the scope of this virus offence.

Moreover, any person who markets or makes accessible passwords, programs or other data that are intended to be used to obtain unauthorised access to a data processing system is liable to a custodial sentence not exceeding three years or to a monetary penalty as prescribed by Article 143bis paragraph 2 SCC.

Finally, exporting or brokering certain goods for monitoring the internet or mobile telecommunications without official permission can be liable to a custodial sentence of up to three years or to a monetary penalty pursuant to Article 9 of the Ordinance on the Export and Brokering of Goods for Monitoring Internet and Mobile Communication.

Identity theft or identity fraud (e.g. in connection with access devices)

There is no explicit regulation for identity theft or identity fraud in Switzerland. Depending on the intention of the offender and his *modus operandi*, it can be covered by different articles of the SCC, such as Article 143 (unauthorised obtaining of data), Article 146 (fraud), Article 147 (computer fraud), Article 143bis (hacking) or Article 173 *et seqq.* (offences against personal honour).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft can be covered by several criminal offences. Article 143 SCC prescribes the penalty for an unauthorised data acquisition. The maximum penalty is a custodial sentence of five years. Furthermore, any person who betrays a manufacturing or trade secret that is not to be revealed under a statutory or contractual duty or anyone who exploits such a betrayal can face a custodial sentence of up to three years or a monetary penalty under Article 162 SCC. Finally, according to Article 67 *et seqq.* of the Swiss Copyright Act, a copyright infringement that has been committed wilfully and unlawfully can be punished with a custodial sentence of up to one year or a monetary penalty; in cases of committing the offence for commercial gain, the penalty is a custodial sentence not exceeding five years or a monetary penalty.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The following further criminal offences impairing security, confidentiality, integrity and availability have to be considered under Swiss law:

- falsification or suppression of information in connection with a telecommunications service (Article 49 of the Swiss Telecommunications Act (TCA)) – penalty: a custodial sentence of up to three years; or a monetary penalty;
- unauthorised misuse or disclosure of information received by means of a telecommunications installation that was not intended for the receiver (Article 50 TCA) – penalty: a custodial sentence of up to one year; or a monetary penalty;
- interfering in telecommunications or broadcasting (Article 51 TCA) – penalty: a custodial sentence of up to one year; or a monetary penalty;
- obstructing, disrupting or endangering the operation of a telecommunication service or utility provider (Article 239 SCC) – penalty: a custodial sentence of up to three years; or a monetary penalty;
- breach of professional confidentiality (Article 321 SCC) – penalty: a custodial sentence of up to two years; or a monetary penalty. Article 35 of the Swiss Federal Act on Data Protection (FADP) – penalty: monetary penalty. Article 47 of the Banking Act – penalty: a custodial sentence of up to three years; or a monetary penalty. Article 147 of the Financial Market Infrastructure Act (FMIA) – penalty: a custodial sentence not exceeding three years; or a monetary penalty;
- breach of postal or telecommunications secrecy (Article 321ter SCC) – penalty: a custodial sentence not exceeding three years; or a monetary penalty. Articles 43 and 53 of the Swiss Telecommunications Act (TCA) – penalty: fine not exceeding CHF 5,000; and
- unsolicited distribution of spam massages (Article 3 *lit*. o in conjunction with Article 23 of the Swiss Federal Law on Unfair Competition) – penalty: a custodial sentence of up to three years; or a monetary penalty.

Failure by an organisation to implement cybersecurity measures

There is no generally applicable regulation in Switzerland specifically requiring the implementation of certain cybersecurity measures (for sector-specific requirements, see question 3.2 below). However, general compliance obligations require the implementation of an internal control system (relevant for companies limited by shares, see Article 20 of the Swiss Code of Best Practice for Corporate Governance) and technical and organisational measures to ensure the confidentiality, integrity and availability of information and IT systems, which can include the implementation of an adequate information security management system (relevant for all organisations, see Article 7 FADP).

The Swiss Federal Council adopted a "National Strategy on Switzerland's Protection against Cyber Risks" (NCS) in 2012. One of the measures provided for in the NCS was the evaluation of existing legislation for immediate adjustment needs. In 2016, the involved authorities declared that they did not detect such need for adjustment of existing legislation from a cybersecurity perspective.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The extraterritorial application of the SCC, with regard to the offences mentioned above, requires that the offender is present in Switzerland and will not be extradited (Articles 6, 7 SCC). In the context of phishing, it is currently in dispute between the Swiss Office of the Attorney General and the criminal courts whether, on the basis of the Council of Europe's Cybercrime Convention in conjunction with Article 6 SCC, such offences committed abroad are even subject to Swiss criminal jurisdiction where the offender and victim are not Swiss citizens.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Yes, Swiss criminal law incorporates the mitigating principles of withdrawal and active repentance. If a person of his own accord does not complete the criminal act or if he assists in preventing the completion of the act, the court may reduce the sentence or waive any penalty (Article 23 SCC).

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

The following other provisions can be applicable in the context of cybersecurity:

- causing fear and alarm among the general public (Article 258 SCC);
- public incitement to commit a felony or act of violence (Article 259 SCC);
- participating in or supporting a criminal organisation (Article 260ter SCC);
- financing terrorism by collecting or providing funds (Article 260^{quinquies} SCC);
- foreign operations and activities directed against the security of Switzerland (Article 266bis SCC);
- diplomatic treason: endangering the interest of Switzerland: (i) by making a secret accessible to a foreign country; or (ii) by falsifying, destroying, disposing or stealing documents relating to Switzerland's legal relations with a foreign state (Article 267 SCC);
- political, industrial or military espionage in the interest of a foreign state or organisation (Articles 272, 273, 274 SCC);
- founding of an unlawful association (Article 275ter SCC); and
- criminal provisions concerning the representation of acts of violence (Article 135 SCC), pornography (Article 197 SCC) or racial discrimination (Article 261bis SCC).

Please note the decisions of the Swiss Federal Criminal Court, SK.2013.39, and the Swiss Federal Supreme Court, BGer 6B_645/2007, both regarding cases of "cyber-jihad/cyber-terrorism", included several of the above-mentioned offences as part of the subject of the accusation.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

- Federal Act on Data Protection.
- Ordinance to the Federal Act on Data Protection.
- Swiss Criminal Code.
- Telecommunications Act.
- Ordinance on Telecommunications Services.
- Federal Act on Copyright and Related Rights.
- Trade Mark Protection Act.
- Civil Code, Code of Obligations.
- Banking Act.
- Ordinance on Banks.
- Financial Market Infrastructure Act.
- Financial Market Supervision Act.
- Federal Law on Unfair Competition.
- Federal Act on the Implementation of International Sanctions.
- Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods.
- Ordinance on the Export, Import and Transit of Dual Use Goods, Specific Military Goods and Strategic Goods.
- Ordinance on the Export and Brokering of Goods for Monitoring Internet and Mobile Communication.
- Federal Act on the Intelligence Service.
- Federal Information Security Act (expected as of 2018).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

In Switzerland, there are no generally applicable mandatory cybersecurity requirements for critical infrastructures so far (for sector-specific requirements, see question 3.2 below). In 2012, the Swiss Federal Council adopted the "National Strategy on the Protection of Critical Infrastructures" (SIK). The Swiss Federal Office for Civil Protection was mandated to implement the strategy and published a "Guideline for the Protection of Critical Infrastructures" in 2015, outlining recommended risk, crisis and continuity concepts based on international standards. Furthermore, the draft bill of a Swiss Federal Information Security Act issued by the Swiss Federal Council in February 2017 prescribes certain security measures for Swiss Federal authorities and offers support to private operators of critical infrastructures to minimise network and system disruptions.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

There is no generally applicable requirement in Switzerland to take measures to monitor, detect, prevent or mitigate Incidents. However, Article 7 FADP in conjunction with Articles 8 and 9 of the Ordinance to the FADP provide that personal data must be protected against unauthorised processing, destruction, loss, technical faults, forgery, theft or unlawful use through the implementation of adequate technical and organisational measures including mandatory controls of the following IT and data-related circumstances: entrance; personal data carrier; transport; disclosure; storage; usage; access; and input.

With regard to specific cybersecurity safeguards to be implemented in the financial and telecommunications sector, see question 3.2 below.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Such conflicts of laws cannot currently be perceived.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

So far, there is no general reporting obligation for cyberattacks in Switzerland. However, a duty to notify the Swiss Federal Data Protection and Information Commissioner in cases of unauthorised data processing or loss of data has been included in the preliminary draft of the revised FADP. Specific reporting obligations are currently only imposed on certain industries such as the financial and the telecommunication sector, see question 3.2 below.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Organisations have the possibility (not the obligation) to inform MELANI, the Swiss Reporting and Analysis Centre for Information Assurance. Such a notification can be filed anonymously with a simple message on MELANI's website. Furthermore, it is also possible to inform the Swiss Coordination Unit for Cybercrime Control (CYCO).

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

There is no such explicit obligation to inform affected individuals under Swiss law. However, in the legal literature, it is partially held that organisations are obligated to report such Incidents to the affected individuals in accordance with Article 4 paragraph 2 FADP, incorporating the principle of good faith. The necessity and extent of such information depends on the circumstances, e.g. the gravity of the breach and the necessity to prevent any damages and potential abuse of the disclosed data. The preliminary draft of the revised FADP provides for obligations to notify affected data subjects in cases of unauthorised data processing or loss of data.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The responses do not change.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The supervisory authorities monitoring and enforcing the above-mentioned requirements pertaining to general data protection and sector-specific cybersecurity are the following:

- Federal Data Protection and Information Commissioner.
- Cantonal Data Protection Commissioners.
- Federal Office of Communications (OFCOM).
- Financial Market Supervisory Authority (FINMA).

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Due to the absence of a general obligation to implement safeguards against cyberattacks or to report Incidents to an authority, there are no penalties for not complying.

For penalties triggered by not complying with sector-specific obligations to report Incidents to the supervisory authorities, see question 3.2 below.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

So far, to our knowledge, the competent supervisory authorities have enforced sector-specific reporting provisions only in cases that had no connection with cybersecurity. However, in 2016, FINMA ordered banks of supervisory category 1 (extremely large, important and complex market participants; very high risk) and category 2 (very important, complex market participants; high risk) to conduct an additional examination and invited those of category 3 (large and complex market participants; significant risk) to conduct a self-assessment pertaining to the status of the implementation of safeguards against cyberattacks.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, market practice varies across business sectors as the legal requirements are different (see question 3.2 below).

In addition, please note that, on 18 April 2018, the Swiss Federal Council adopted "The National Strategy for the Protection of Switzerland against Cyber Risks" which will certainly impact all sectors in Switzerland.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

(a) Yes, Article 14 of the Financial Market Infrastructure Act (FMIA) requires financial market infrastructures (*i.a.* stock

exchanges, trading facilities, payment systems) to operate robust IT systems which are appropriate for their activities, provide for effective emergency arrangements, ensure the continuity of the business activity, and provide for measures to protect the integrity and confidentiality of information regarding their participants and their transactions. Article 3f of the Banking Act and Article 12 paragraph 4 of the Ordinance on Banks require banks to implement appropriate risk management, including an internal control system, in order to detect, limit and monitor, *i.a.*, relevant operational risks. These requirements are specified in the recently updated FINMA Circular 2008/21 "Operational Risks – Banks" where the minimum details of a cyber risk management concept to be implemented based on international standards are outlined (protection of processes/IT systems/sensitive data, detection and recording of cyberattacks, remedial measures, recovery of normal operations, regular vulnerability analysis and penetration testing). FINMA Circulars are not legally binding, but they elaborate the regulator's intended enforcement practice and are regularly accepted and complied with by the industry.

According to Article 29 paragraph 2 of the Financial Market Supervision Act (FINMASA), FINMA has to be informed about any Incident that is of substantial importance to the supervision, which can include Incidents that could have a negative impact on the reputation or operation of the financial institution or the financial centre of Switzerland. Pursuant to Articles 45 and 46 FINMASA, the wilful provision of false information to FINMA or failing to make a mandatory report to FINMA can be punished with a custodial sentence of up to three years or a monetary penalty, and in cases of negligence with a fine of up to CHF 250,000. In case of a serious infringement of the supervisory provisions, the licence of a supervised person or entity can, according to Article 37 FINMASA, be revoked, its recognition withdrawn or its registration cancelled.

(b) On the basis of Article 96 paragraph 2 of the Ordinance on Telecommunications Services (OTS), OFCOM has published a currently non-binding "Guideline on Security and Availability of Telecommunications Infrastructures and Services" recommending telecommunications service providers to implement, monitor and update (i) an information security management system as described in the international standards relating to information security, such as ISO/IEC 27001:2005 and ITU-T X.1051, (ii) a business continuity plan, and (iii) a disaster recovery plan, and to comply with international security recommendations in the ICT sector, such as the "ETSI White Paper No. 1 – Security for ICT" and the "ITU-T ICT Security Standards Roadmap". OFCOM has the competence to declare the mentioned guideline to be binding.

Article 96 OTS prescribes the obligation of telecommunications service providers to immediately inform OFCOM of disruptions in the operation of their networks which (potentially) affect at least 30,000 customers (landline, over-the-top, broadcasting) or 25 transmitter sites (mobile communications). OFCOM requires the operators to include in the report, *i.a.*, a description of the disruption, the categories of causes (cable rupture, energy/hardware/software/human failure, cyberattack, malicious interference) and the measures taken to end the disruption. Pursuant to Article 53 of the Telecommunications Act, anyone who infringes any provision of the telecommunications legislation, such as the reporting obligation under Article 96 OTS, is liable to a fine not exceeding CHF 5,000.

Finally, there are further sector-specific requirements, particularly in connection with aviation, the railway industry and nuclear energy.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

If the failure results from not having an adequate compliance management system (including risk management, internal reporting and control, and sufficient supervision) in a company limited by shares or a limited liability company, this can constitute a breach of the directors' obligation to perform their duties with all due diligence and to safeguard the interests of the company in good faith (Articles 717, 812 Code of Obligations) and to supervise the persons entrusted with managing the company, in particular with regard to compliance with the law (Article 716a Code of Obligations). These duties are only explicitly imposed on members of the board of directors, managing directors and executive officers of companies limited by shares, and managing directors of limited liability companies.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) There is no such general obligation to designate a CISO under Swiss law.

(b) Apart from special sector-related requirements (see question 3.2 above), there is no such general obligation to establish a written Incident response plan or policy.

(c) Apart from special sector-related requirements (see question 3.2 above), there is no such general obligation to conduct periodic cyber risk assessments, including for third-party vendors.

(d) Apart from special sector-related requirements (see question 3.2 above), there is no such general obligation to perform penetration tests or vulnerability assessments.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no generally applicable disclosure requirements in relation to cybersecurity risks or Incidents for companies in Switzerland (for sector-specific requirements, see question 3.2 above). However, if an Incident can result in damage claims or penalties, these risks have to be assessed and appropriate provisions have to be established and included in the balance sheet in the annual reports.

Furthermore, in the event that a large number of data subjects are affected, there may be an exceptional duty to report the Incident publicly according to the data procession principle of good faith (see question 2.7 above). This can particularly be the case if the data subjects concerned cannot be informed individually.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

There are no other specific requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

According to Article 15 paragraph 1 FADP in conjunction with Article 28 *et seqq*. of the Swiss Civil Code, the affected person of a cybercrime-induced data breach has the possibility to bring actions relating to the protection of privacy, provided that there is a violation of personality rights, e.g. due to data theft or illegal data processing. This can include actions for damages, prohibitive injunctions, information/disclosure and notification of third parties or the publication of judgments. Furthermore, members of the board of directors, managing directors and executive officers of companies limited by shares and managing directors of limited liability companies are liable both to the company and to the individual shareholders and creditors, for any losses or damage arising from any intentional or negligent breach of their duties (Articles 754, 827 Code of Obligations); see question 4.1 above.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

To date, we are not aware of any civil actions that have been filed by affected persons or companies in relation to cybersecurity Incidents in Switzerland. The few judgments pertaining to liability for data breaches derive from administrative investigations conducted by the supervisory authorities.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

If the claimant is able to prove damages and the violation of a legally protected right or norm, the purpose of which is to protect from such damages, he is entitled to compensation for moral sufferings and the payment of damages by virtue of Articles 49 and 41 of the Code of Obligations. Furthermore, according to Article 423 of the Code of Obligations, data subjects can request the handing over of profits arising from violations of their privacy rights.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Since 2000, organisations have the possibility to take out insurance against cyberattacks. The offered coverage includes, for example, the loss or theft of data, damages due to hacking and malware, and the unauthorised disclosure of data.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations to insurance coverage concerning such Incidents.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

(a) There are no such specific requirements.

(b) A general reporting obligation of cyber risks and other potential Incidents for employees *vis-à-vis* the employer can, according to Article 321a of the Code of Obligations, be derived from the duty of care and loyalty.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

Laws with possibly inhibiting effects on reporting cyber risks and similar Incidents could be triggered by the secrecy provisions mentioned under the last heading of question 1.1 above. Furthermore, in Switzerland, there is no explicit protection for whistleblowers, so far, who report Incidents with regard to their employers to public authorities or the media. However, a draft bill of the Code of Obligations, which is still under the scrutiny of the legislative institutions, introduces such whistleblower protection from termination and other detriments (Article 336 paragraph 2 *lit*. d, Article 328 paragraph 3 Code of Obligations).

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

KOBIK, the Swiss Coordination Unit for Cybercrime, does not only function as a notification office for cybercrimes, but also looks actively for criminally relevant content on the internet. However, after its verification, KOBIK passes the information to the competent criminal law enforcement authorities, which are the local, cantonal and Swiss Federal police departments and public prosecutors' offices.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no such requirements under Swiss law.

Dr. András Gurovits
Niederer Kraft Frey Ltd.
Bahnhofstrasse 53
CH-8001 Zurich
Switzerland

Tel: *+41 58 800 80 00*
Email: *andras.gurovits@nkf.ch*
URL: *www.nkf.ch*

András Gurovits specialises in technology (IT, telecoms, manufacturing, regulatory) transactions (including acquisitions, outsourcing, development, procurement, distribution), data protection, corporate, dispute resolution (incl. administrative proceedings) and sports.

He regularly advises clients on contractual, compliance, governance, disputes and other legal matters in the above areas.

He, thus, not only advises in these areas, but also represents clients before the competent regulatory and investigating authorities, state courts and arbitral tribunals.

Dr. Gurovits is distinguished as a leading lawyer by various directories such as *Chambers* and *The Legal 500*. Dr. Gurovits has been a lecturer at the University of Zurich for more than a decade. Presently, he is a listed arbitrator with the Court of Arbitration for Sport (CAS/TAS) in Lausanne and member of the Legal Committee of the International Ice Hockey Federation.

Clara-Ann Gordon
Niederer Kraft Frey Ltd.
Bahnhofstrasse 53
CH-8001 Zurich
Switzerland

Tel: *+41 58 800 80 00*
Email: *clara-ann.gordon@nkf.ch*
URL: *www.nkf.ch*

Clara-Ann Gordon is specialised in the areas of TMT/outsourcing, data privacy, internal investigations/e-discovery and compliance. She regularly advises clients in the above areas on contractual, governance/compliance and other legal matters, represents clients in transactions and before the competent regulatory and investigating authorities as well as before state courts, arbitral tribunals and in mediation proceedings, and renders opinions on critical regulatory and contract law topics in the said industry-specific areas.

She has advised on and negotiated a broad range of national and international IT, software and outsourcing transactions (also in regulated markets), has represented clients in technology-related court proceedings and international arbitration, and is experienced in data protection and secrecy laws, white-collar investigations and e-discovery, telecom regulations (including lawful interception), e-commerce, and IT law.

Ms. Gordon regularly publishes in the field of technology (ICT) and frequently speaks at national and international conferences on emerging legal issues in technology law.

NIEDERER KRAFT FREY

Established in 1936, Niederer Kraft Frey Ltd. is a preeminent Swiss law firm with a proven track record of legal excellence and innovation.

Throughout our history, we have continuously worked on the most important and demanding cases entrusted to Swiss law firms. This is the foundation of our distinct market knowledge, expertise and experience as well as our capacity for innovative thought.

We work and think internationally. As a market leader in Switzerland, we have built long-standing relationships with the world's best international law firms. The majority of our lawyers have undertaken further training at American, British or other foreign universities and many of us have gained professional experience in partner law firms abroad.

Thanks to our heritage and market position we offer innovative and sustainable services, and avoid being influenced by short-term trends. We attach great importance to combining a highly professional approach and persistence in pursuing our clients' goals with being easy to work with, even in the most demanding situations.

Taiwan

Sean Yu-Shao Liu

Lee, Tsai & Partners Attorneys-at-Law

Sophia Ming-Chia Tsai

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Offences against computer security are generally regulated by the Criminal Code of the Republic of China (the "Criminal Code").

Hacking (i.e. unauthorised access)

According to Article 358 of the Criminal Code, a person who accesses, without authorisation, another person's computer or related equipment by entering their account details and password, hacking computer security measures, or exploiting vulnerabilities in computer systems, will be sentenced to imprisonment for not more than three years; in *lieu* thereof, or in addition thereto, a fine of not more than NT$300,000 may be imposed.

Denial-of-service attacks

A person who, without any justification, interferes with another person's computer and other equipment through a computer program or other electromagnetic method, which then causes injury to the public or others, will be sentenced to imprisonment for not more than three years; in *lieu* thereof, or in addition thereto, a fine of not more than NT$300,000 may be imposed (see Article 360 of the Criminal Code).

Phishing

A typical phishing attempt may take the following form:

(1) a person who digitally masquerades as a reliable and famous entity or person in order to obtain another person's account and password; and

(2) such person uses the account and password to obtain, delete or alter the electromagnetic records of the victim and cause injury to the public or others.

The conduct above would first constitute forgery and use of false electromagnetic records, under which the offender will be sentenced to imprisonment for not more than five years (see Articles 210, 216 and 220 of the Criminal Code).

Secondly, the conduct above may constitute a violation of Article 359 of the Criminal Code, under which a person who, without any justification, obtains, deletes or alters the electromagnetic records of another and thus causes injury to the public or others will be sentenced to imprisonment for no more than five years; in *lieu* thereof, or in addition thereto, a fine of not more than NT$600,000 may be imposed.

Further, if the electromagnetic records above involve another person's property, meaning that the phisher unlawfully acquires such property through the false creation, deletion and alteration of records, it would also constitute computer fraud and the offender will be sentenced to imprisonment for no more than seven years; in addition thereto, a fine of not more than NT$700,000 may be imposed (see Article 339-3 of the Criminal Code).

Lastly, if the fraud is conducted through electronic communication or other broadcasting media and directed at the public, the offender may be sentenced to imprisonment for at least one year and no more than seven years; in addition thereto, a fine of not more than NT$1 million may be imposed (see Article 339-4 of the Criminal Code).

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

This would fall under denial-of-service attacks that are punishable under Article 360 of the Criminal Code, as stated above.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Simply possessing such hardware, software or tools for research without causing harm to another does not constitute a crime. However, the use of such hardware, software or tools to interfere with the computer of another and cause injury to the public or another may violate Article 360 of the Criminal Code, as stated above.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity theft

Depending on the facts, identify theft may fall under a violation of Articles 358 and 359 of the Criminal Code, as stated above, which prohibit the use of another's account and password and obtaining/deleting/altering another's electromagnetic records without justification.

Identity fraud

Depending on the facts, identify fraud may violate the aforementioned Articles 210, 216 and 220 of the Criminal Code for forgery of electromagnetic records, or the aforementioned Article 339-3 of the Criminal Code for the unlawful acquisition of another's property and interest by manipulating the electromagnetic records of such property and interest. Further, if the fraud is directed to the public through electronic communication or other broadcasting media, it may also involve a violation of Article 339-4 of the Criminal Code.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Depending on the facts, electronic theft may violate the aforementioned Article 359 of the Criminal Code, which prohibits obtaining, deleting or altering electromagnetic records without justification.

Criminal copyright infringement is provided under Article 91 of the Copyright Act, which carries a sentence of imprisonment for not more than three years' detention, or, in *lieu* thereof, or in addition thereto, a fine of not more than NT$750,000.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Producing malicious code or a program that is directed at committing any of the above activities, the offences which fall under the scope of Articles 358 and 359 of the Criminal Code, or the provision of such code or program to another for the same, is punishable under Article 362 of the Criminal Code and may be punished by imprisonment for not more than five years; in *lieu* thereof, or in addition thereto, a fine of not more than NT$600,000 may be imposed.

Failure by an organisation to implement cybersecurity measures

Unless relevant facts correspond to the elements of the aforementioned offences, failure by an organisation to implement cybersecurity measures is not a crime.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Except for Article 339-4 of the Criminal Code, the other aforementioned articles do not have extraterritorial application. Jurisdiction-wise, however, as long as either the conduct or the result of an offence takes place in Taiwan, it is deemed to be an offence that occurred in Taiwan and may be punishable under Taiwan law (see Article 4 of the Criminal Code).

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

If the attackers voluntarily turn themselves in for an offence not yet discovered, the punishment may be mitigated (see Article 62 of the Criminal Code).

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

A person who, with the intention to gain illegal interests or to impair the interests of another, collects, processes or uses personal information in violation of relevant provisions of the Personal Information Protection Act ("PIPA") (mainly Articles 6, 15, 16, 19 and 20), may be sentenced to imprisonment for a term of not more than five years; in addition thereto, a fine of not more than NT$1 million may be imposed (see Article 41 of PIPA).

As many personal data are stored on computers or the internet, when such personal data are leaked as a result of cyber hacking, it usually involves violation of the aforementioned provisions of PIPA and the Criminal Code at the same time. There have been many such instances in Taiwan.

Additionally, a person who, with the intention to endanger national security or social stability, collects or delivers any classified document, picture, information or article to a foreign country or Mainland China may be sentenced to imprisonment for a term of not more than five years; in addition thereto, a fine of not more than NT$1 million may be imposed (see Articles 2-1 and 5-1 of the National Security Act). Further, a person who reveals or delivers information that has been classified under the Classified National Security Information Protection Act ("CNSIPA") may be imprisoned for one to seven years (see Article 32 of CNSIPA).

While the law has contemplated that the above acts may be carried out through a cybersecurity attack on government facilities, there have not been any significant prosecutions in this regard.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The two most important laws concerning cybersecurity in Taiwan are PIPA and the Information and Communication Security Management Act ("ICSM"), the latter of which was just passed by the Legislative Yuan (the lawmaking body in Taiwan) in May 2018 and will soon enter into effect.

ICSM directly concerns the monitoring, detection, prevention, mitigation and management of cybersecurity Incidents and applies to government agencies, providers of critical infrastructure, state-controlled enterprises and state-financed foundations.

PIPA covers how personal data may be collected, stored and used. A company collecting personal data is required to establish a plan to secure such personal data. Further, gaining unauthorised access to a system for stealing personal data may also be found to be a PIPA violation and carry an imprisonment sentence of up to five years.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

ICSM requires providers of critical infrastructure to lay out and implement a cybersecurity maintenance plan. Please see question 2.3 below for details.

Critical infrastructure is defined under ICSM as tangible or virtual assets, systems or networks which may have a major impact on national security, public interest, national livelihood or economic activities should they cease to function or become less effective.

Providers of critical infrastructure will be named by each competent authority in charge of different industries ("Competent Authority") and then approved by the Executive Yuan.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

ICSM requires providers of critical infrastructure, state-controlled enterprises and state-funded foundations ("Regulated Private Entities") to take the following measures:

- Meet the requirements of its cybersecurity rank, which will be stipulated by the Executive Yuan.
- Lay out, amend and implement a cybersecurity maintenance plan in accordance with the type, quantity and nature of the information being kept and processed, as well as the scale and nature of the information and communication system ("Cybersecurity Maintenance Plan").
- Submit a correcting report to its Competent Authority should there be any deficiency that is found in implementing its Cybersecurity Maintenance Plan.

Additionally, PIPA requires all non-government entities that keep personal information to adopt appropriate security measures to prevent such information from being stolen, tampered with, damaged, lost or leaked.

Relatedly, Competent Authorities may designate specific companies to lay out and implement a security maintenance plan for the personal information that they possess. For instance, the National Communications Commission ("NCC") and the Financial Supervisory Commission ("FSC") have ordered telecommunications/broadcasting companies and certain financial institutions, respectively, to set up and implement such a plan.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

We have not found any conflict of law issues in relation to the requirements mentioned above.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Under ICSM, Regulated Private Entities must establish a notification and contingency mechanism in response to Incidents.

As soon as it learns of an Incident, the Regulated Private Entity must notify its Competent Authority of the Incident and subsequently submit a report explaining how it has investigated and handled the Incident and what it has done to make improvements as well as the result of these improvements. The report must also be submitted to the Executive Yuan if the Incident is significant.

Details of the above mechanism are pending in the Executive Yuan.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

There is no law or regulation prohibiting organisations from voluntarily sharing information related to Incidents or potential Incidents with any entities. Nevertheless, the disclosure must comply with other applicable laws, such as PIPA.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

If an Incident involves unauthorised access, disclosure or alteration of personal data, the organisation must notify the affected individuals of the infringement and the measures in response taken in accordance with PIPA. While ICSM is also expected to have similar disclosure requirements once it is promulgated, the scope of such disclosure is currently unknown.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No. The answers to questions 2.5 to 2.7 remain the same.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Executive Yuan and the Competent Authorities of each specific industry are responsible for the enforcement of ICSM. The Executive Yuan is mainly responsible for the lawmaking part of the policies and regulations, while the Competent Authorities of each industry are at the frontline of enforcing ICSM.

As stated above, the Competent Authorities will be responsible for naming the critical infrastructure providers as well as drafting rules regarding the Cybersecurity Maintenance Plan, with oversight and approval by the Executive Yuan. The Competent Authorities are also responsible for conducting inspections to see whether companies are diligently implementing their respective Cybersecurity Maintenance Plans.

As for PIPA, under most circumstances, both Competent Authorities and local governments have the power to implement PIPA.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

If the providers of critical infrastructure fail to comply with their obligations under ICSM, such as implementing the Cybersecurity Maintenance Plan, conducting regular reviews, submitting improvement reports, and establishing the notification and contingency mechanisms, the Competent Authority will order such provider to take corrective measures within a specified time period. Failure to do so will result in an administrative fine of no less than NT$100,000 but no more than NT$1 million for each violation.

If a provider of critical infrastructure fails to notify the Competent Authority and/or the Executive Yuan regarding the occurrence of an Incident, such provider will be fined no less than NT$300,000 but no

more than NT$5 million and be ordered to take corrective measures within a specified time period. Failure to take such corrective action will result in additional administrative fines for each violation.

If a non-government entity fails to notify the subjects of an infringement to their personal information in violation of PIPA, the relevant Competent Authority or the county or city government will order such entity to take corrective measures within a specified time period. Failure to take such corrective action will result in administrative fines of no less than NT$20,000 but no more than NT$200,000 for each violation.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

First Bank: ATM Hacking

In 2016, First Bank in Taiwan reported that 41 of its ATMs were hacked and NT$83.27 million in cash was stolen. Afterwards, First Bank was found to have several information security vulnerabilities, such as failing to isolate the ATM administration server or implementing appropriate security measures for its voice-mail system at its London branch, which was the point of intrusion. This was found to be in violation of the "Guidelines for Financial Institutions on Information Security Management in Electronic Banking" regarding the use of isolated networks and antivirus software.

First Bank was found to have also failed to allow security experts to audit its records for unauthorised access, which is a violation of the "Guidelines for Financial Institutions on the Assessment of Information Security for Computer Systems" regarding the obligation to review network and server access records for irregularities and verify warning systems. For the above omissions, the FSC imposed a fine of NT$10 million on First Bank for violation of Article 45-1 of the Bank Act.

Far Eastern Bank: SWIFT System Hacking

In 2017, Far Eastern International Bank in Taiwan reported that its SWIFT system had been infected with viruses, which allowed hackers to steal more than NT$1.8 billion. According to the FSC's investigation, Far Eastern International Bank was found to have been negligent in maintaining its SWIFT system because it failed to properly establish or implement an internal control system for information security; notably, the SWIFT system server was not properly isolated from the network, and administrator access was too broad and not properly managed. For the above omissions, the FSC imposed a fine of NT$8 million on Far Eastern for its violation of Article 45-1 of the Bank Act.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

While the financial industry in Taiwan is generally known for having the most developed information security systems, the occurrence of the above Incidents, noted in question 2.11, indicates that when it comes to proactively maintaining security concepts in practice, Taiwan companies as a whole still have significant room for improvement in terms of information and network security.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

(a) The financial services sector

Financial institutions are required to follow certain security standards stipulated by the Bank Association and approved by the FSC for their information systems, and they are obliged to inform the FSC and the Central Bank of any cybersecurity Incident that may affect their business operations or infringe on the interests of their customers.

Private financial institutions have to report to the FSC, the Central Bank and the Central Deposit Insurance Corporation any cybersecurity Incident that may affect their business operations or infringe on the interests of their customers. For state-run financial institutions, they have to report to the Ministry of Finance, FSC, etc.

The contents of the report must include the time of the Incident, the relevant data involved, the level of impact, the events of the Incident, the type of Incident, and emergency measures taken. There are no exceptions to this reporting obligation.

In response to increasingly prevalent cyberattacks, the FSC has required banks to set up a separate department in charge of information security before September 2018.

(b) The telecommunications sector

Telecommunications companies are required by the NCC to stipulate and implement an information security plan, which must cover information security management standards, the assessment of cybersecurity levels, the mechanisms for managing information security, and the response and notification mechanisms, etc. The contents and process of the report are similar to those for financial institutions, save for the fact that the competent authority is the NCC instead of the FSC.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

According to Article 23 of the Company Act, the responsible person of a company (e.g., director or manager) must be loyal to the company and must exercise the due care of a good administrator in conducting the business operations of the company.

If the director or manager is also responsible for a company's information security matters, and he or she intentionally or negligently failed to follow the relevant cybersecurity requirements so as to prevent, mitigate, manage or respond to an Incident, it is very likely that such responsible director or manager will be held personally liable under Article 23 of the Company Act for failing to exercise due care.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) ICSM provides that Regulated Private Entities of a certain cybersecurity rank or higher must have personnel exclusively dedicated to information security.

Currently, banks and insurance companies are required by the FSC to set up a dedicated cybersecurity unit, designate a high-level manager, and allocate sufficient resources to deal with relevant cybersecurity matters.

(b) ICSM provides that Regulated Private Entities must establish a notification and contingency mechanism to respond to Incidents. Additionally, as stated above in question 2.3, financial institutions and telecommunication companies, etc., are required by the Competent Authorities, pursuant to PIPA, to establish and implement a security maintenance plan for the personal information that they possess. The said plan must include a notification and contingency mechanism to handle Incidents involving leaks of personal information.

(c) Periodic cyber risk assessments

ICSM requires periodic review of how Regulated Private Entities implement their maintenance plans for information security. The frequency and other details are yet to be announced. In addition to ICSM, certain Competent Authorities have the power to require companies in their respective industries to perform periodic cyber risk assessments.

For example, financial institutions are required by the FSC to conduct periodic risk assessments depending on the classification of their computer systems and their evaluation cycles; in the telecommunications industry, the NCC requires telecommunications companies to carry out periodical internal audits, which include network security.

(d) Penetration tests or vulnerability assessments

It remains to be seen whether and how Regulated Private Entities would be required to conduct penetration tests or vulnerability assessments under ICSM, but the FSC and the NCC are again frontrunners in this regard: financial institutions are required to conduct penetration tests for their own websites and scan and repair vulnerabilities in their network equipment, servers and terminal equipment; telecommunications companies must conduct penetration tests, vulnerability scanning, and maintenance and repairs on a regular basis.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Regulated Private Entities

Please see the response to question 2.5 above for the proposed rules under ICSM, details of which will be further determined by the Executive Yuan.

Financial institutions

Financial holding companies or banking businesses must assess and review the status of their internal control systems (which covers information and communications security), submit statements regarding such systems, and publish the information contained in those statements on the company's website as well as a website designated by the competent authority within three months of the end of each fiscal year. The internal control systems statement must be included in the annual report and prospectuses.

Telecommunications companies

The NCC has requested telecommunications companies to submit a self-assessment of their operational security levels to the NCC before the end of September each year. However, this is not a mandatory requirement.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

As stated above, depending on the industry, a company in Taiwan may be subject to regulations or practices which may be connected to cybersecurity concerns (if at all).

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In the event of any Incident, the victim will most likely bring a civil action against the offender under the relevant provisions of the Civil Code of Taiwan.

A person who, intentionally or negligently, infringed on the right of another is liable for any injury arising therefrom (see Article 184, first half of Paragraph 1 of the Civil Code). In the event that the infringement violates ethics or laws protecting another (such as the aforementioned Articles 358, 359, 360 and 362 of the Criminal Code), this "right" of a person could be interpreted broadly and includes not only statutory rights, but also a person's economic interests or his/her personality rights, which are particularly relevant in the context of many Incidents because often there may be no physical damage to the victim (see Article 184, second half of Paragraph 1, and Paragraph 2 of the Civil Code). For example, in a denial-of-service attack, the victim's property is sound but the victim's business operations might be completely shut down.

In the event of an infringement of a personality right in an Incident, the victim may request the court to remove the infringement while also claiming monetary damages; if the victim's reputation has been damaged, the offender must take proper measures to rehabilitate the victim's reputation (see Articles 18 and 195 of the Civil Code).

Additionally, for an Incident involving personal data, the victim may also be able to claim against the entity collecting or storing such data if the injury may be attributed to the entity's failure to implement proper security measures or comply with any other provision of PIPA in handling personal data (Articles 29 and 30 of PIPA).

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

ATM hacking (the First Bank case)

Regarding the aforementioned First Bank ATM hacking case, although the key perpetrators are unknown foreign individuals abroad and thus practically unfeasible to bring to justice in Taiwan, the three individuals who were physically manipulating the hacked ATMs to withdraw money were caught and sentenced with imprisonment ranging from four years and six months to four years and 10 months pursuant to Article 359 of the Criminal Code (altering the electromagnetic records of another).

Notably, although the final sentences are almost at the maximum statutory time (five years), the judges suggested in the decision that legislators need to set greater punishments to cope with these new types of offences (see 106-Shang-Su-Zi-593 Criminal Decision). It remains to be seen whether the suggestion and the prevalence of more serious cyber crime would facilitate the amendment of the relevant provisions of the Criminal Code.

Altering electromagnetic records of online games

In the 103-Tai-Shang-Zi-3093 Criminal Decision, the defendant was accused of exploiting a vulnerability in an online game distributed by the plaintiff company to enable the use of external software for running multiple accounts and for selling in-game items for real money. The court found the defendant's conduct as having damaged the plaintiff's business interest and management of its electromagnetic records in the form of such "in-game items", which constitute the offence of altering electromagnetic records of another under Article 359 of the Criminal Code.

In the civil case arising from the above, the court reasoned that Article 359 of the Criminal Code, in essence, sets out a right (i.e., the integrity of electromagnetic records) to be protected, which falls under Paragraph 2 of Article 184 of the Civil Code regarding a "law to protect another". Therefore, a victim may claim civil compensation from the perpetrator of an offence, under Article 359 of the Criminal Code, by citing a breach of a provision protecting the rights of another under Paragraph 2 of Article 184 of the Civil Code.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

As stated above, relevant articles of tort in the Civil Code of Taiwan are the main basis to bring civil actions in reference to Incidents.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. The insurance industry in Taiwan has launched several information security-related policies on the market, which may be generally split into the following categories:

- Security and Privacy Insurance

  Depending on the insurer, the scope of the policies may cover the costs of handling cyber attacks (such as forensic analysis and legal consulting), liabilities arising from disclosure of personal information, revenue loss of business due to cyber attacks, etc.
- Information System Insurance (for financial institutions)

  This insurance is exclusively designed for financial institutions to cover their losses arising from the illegal alteration or destruction of electronic records due to cyber attacks.
- Information Products/Services Liability Insurance

  This insurance covers liabilities of companies whose inadequate IT products or services were determined to play a key part in the Incident.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Currently, no such regulatory limitations to insurance coverage against information security-related events have been imposed. However, as information security-related insurance is considered a form of property insurance, all the regulations regarding property insurance should still be complied with, such as the "Autonomous Regulations on Designing Property Insurance Products" regarding the requirement to clearly specify the scope of the policy, and the scope must be mutually commensurate with the stipulated premium rates.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

(a) The monitoring of employees for information security-related purposes is allowed, as long as the general rules for monitoring employees are complied with. Past judicial decisions have held that employers may monitor employees if 1) the employee monitoring policy was disclosed beforehand, 2) the employee consents in writing to be monitored, 3) there is a reasonable basis to suspect that monitoring could result in collection of work-related evidence or offence, and 4) for work-related monitoring, there is a reasonable causal link between the method used and the purpose to be achieved. Violation of any of the above may be deemed as a breach of the employee's privacy.

(b) There is no specific obligation under Applicable Law on employees for reporting cyber risks, security flaws, Incidents or potential Incidents to the employer. However, the employer's internal rules may impose such a reporting obligation on the employee, which must be reasonable and necessary so as to be binding against the employee. Nevertheless, with the relevant implementation rules of ICSM to be soon promulgated by the Executive Yuan and Competent Authorities, it remains to be seen whether those rules will specifically impose reporting obligations on employees of Regulated Private Entities.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No such limitations in whistle-blowing laws exist as of now. However, if the reporting of such matters resulted in the disclosure of company secrets or other confidential information, the employee could be held liable for compensation of any damages caused as a result. The upcoming implementation rules of ICSM may make changes in this regard.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Criminal investigations

If an Incident involves a criminal offence, the prosecutor or the police (after being approved by a prosecutor) may apply to the court for a search warrant to search the property, electronic records, dwelling, or other premises of an accused person or a suspect.

Administrative investigation

ICSM provides that Competent Authorities ***must*** periodically inspect the providers of critical infrastructure for how their Cybersecurity Maintenance Plans are implemented and ***may*** do so to the other types of Regulated Private Entities.

Although the details of this inspecting power have yet to be set out, we do not expect it to be extensive because an even broader investigation power was contemplated during the legislative process

of ICSM, but later deleted from the final draft due to a failure to reach consensus among the lawmakers on the matter.

That said, in certain highly regulated industries (such as finance and telecommunications), the respective authorities have strong powers to initiate and conduct administrative investigations.

For example, in the aforementioned ATM heist case, the FSC, as a bank authority, investigated whether First Commercial Bank was negligent in maintaining its ATM system. Such investigative power is derived from Article 45 of the Banking Act, which provides that the FSC may appoint a designee or entrust an appropriate institution to examine the business, financial affairs and other relevant affairs of a bank or related parties, or direct a bank or related parties to prepare and submit, within a prescribed period of time, balance sheets, property inventories or other relevant documents for examination.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There is no requirement to implement law enforcement backdoors under Applicable Laws in Taiwan.

Sean Yu-Shao Liu
Lee, Tsai & Partners Attorneys-at-Law
9th Fl., 218 Tun Hwa S. Rd.
Sec. 2, Taipei 106
Taiwan

Tel: +886 2 2378 5780
Email: seanliu@leetsai.com
URL: www.leetsai.com

Sean is an associate partner at Lee, Tsai and Partners Attorneys-at-Law. He is an experienced litigator and has acted for clients from the government to major companies, domestic and abroad.

Sean works on a wide variety of legal issues and specialises in construction, antitrust, unfair competition and commercial disputes. He frequently represents clients before the civil courts, administrative courts, the Fair Trade Commission, the China Arbitration Association and Complaint Review Board for Government Procurement.

With an extensive understanding of technology and business, Sean advises many major companies in corporate legal matters, such as fundraising, M&A, joint venture, licensing, procurement, distribution and agency. Beside his legal practice, Sean is active in public discussion of legal policy, notably laws and regulations involving financial technology and start-up fundraising. He is now a member of the Taiwan Fintech Association.

Sophia Ming-Chia Tsai
Lee, Tsai & Partners Attorneys-at-Law
9th Fl., 218 Tun Hwa S. Rd.
Sec. 2, Taipei 106
Taiwan

Tel: +886 2 2378 5780
Email: sophiatsai@leetsai.com
URL: www.leetsai.com

Sophia is an associate at Lee, Tsai and Partners Attorneys-at-Law. Her practice focuses on general corporate legal affairs, general civil and criminal law, e-commerce, and cryptocurrency. She is also a member of the Taiwan Fintech Association and participates in discussion of legal amendments. She is currently engaged in learning about innovative technologies, such as AI, blockchain, cryptocurrency, driverless vehicles, virtual reality and augmented reality.

理慈 Lee, Tsai & Partners
A GREATER CHINA LOCAL FIRM

Dr. Chung-Teh Lee and Jaclyn Tsai founded the first office of the Lee Tsai Group in Taipei in 1998 with the professional motto "Reason and Compassion" and expanded to Shanghai in 2001 and Beijing in 2010. The firm's Tech/IP Practice is led by Ms. Jaclyn Tsai, who, during her appointment as Minister without Portfolio, was responsible for cybersecurity-related issues in e-commerce-related laws and the convening of the Mobile Broadband Service and Industry Development Taskforce; she also sat on the National Information and Communication Security Taskforce and the Cyber Security Management Law deliberation group. After her term as Minister without Portfolio, Ms. Tsai was elected and currently serves as the Executive Supervisor and Convener of Legal Environment Committee of the Taiwan Fintech Association. She specialises in fintech laws and regulations with a focus on blockchain technology and the self-regulation of initial coin offerings. Ms. Tsai is one of the promotors of the Global ICO Transparency Alliance and the Taiwan Crypto Blockchain Self-Regulatory Organization.

Main Areas of Practice

- Intellectual Property Law.
- Infrastructure Projects / Construction Law.
- Mergers and Acquisitions / Global Investment.
- Dispute Resolution.
- Media and Entertainment.
- Capital Market / Securities.
- Patent Registration / Prosecution.
- Trade Mark Registration.
- Blockchain / ICOs.

Thailand

Saroj Jongsaritwang

R&T Asia (Thailand) Limited

Sui Lin Teoh

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

The main laws and regulations relating to computer crimes in Thailand are the Computer Crime Act 2007 ("**CCA**") and the Thai Penal Code.

Hacking (i.e. unauthorised access)

Yes. Section 5 of the CCA provides that whoever illegally accesses a computer system that has specific security measures and such security measures are not intended for that person's use would be liable to imprisonment not exceeding six months or to a fine not exceeding THB 10,000, or both.

Section 7 of the CCA provides that whoever illegally accesses computer data that has specific security measures which are not intended for that person's use would be liable to imprisonment not exceeding two years or to a fine not exceeding THB 40,000, or both.

Denial-of-service attacks

Yes. Section 10 of the CCA provides that whoever illegally acts in a manner that causes suspension, deceleration, obstruction or interference to a computer system of another person so that it is not capable of functioning normally would be liable to imprisonment not exceeding five years or to a fine not exceeding THB 100,000, or both.

Phishing

Yes. Section 14(1) of the CCA provides that whoever dishonestly or deceitfully inputs into a computer system computer data which is distorted or forged, either in whole or in part, or computer data which is false, in such a manner likely to cause injury to the public (but not constituting a crime of defamation) under the Penal Code, would be liable to imprisonment not exceeding five years or to a fine not exceeding THB 100,000, or both.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. Section 9 of the CCA provides that whoever illegally acts in a manner that damages, impairs, deletes, alters or makes additions to, either in whole or in part, computer data of another person would be liable to imprisonment not exceeding five years or to a fine not exceeding THB 100,000, or both.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

No. However, the Thai Court has the power to forfeit any property used or in possession for use in the commission of an offence by any person.

Identity theft or identity fraud (e.g. in connection with access devices)

No. There is no specific offence in relation to identity theft or identity fraud. However, identity theft/fraud would be considered as the act of causing damage to the computer data of another person under Section 9 of the CCA mentioned above. In addition, whoever inputs into a publicly accessible computer system computer data that will appear as an image of another person and the image has been created, edited, appended or adapted by electronic means or whatsoever means, and in doing so is likely to impair the reputation of such other person or exposes such other person to hatred or contempt, would be liable to imprisonment not exceeding three years and a fine not exceeding THB 200,000, or both (Section 16 of the CCA).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

This is not applicable in our jurisdiction.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Yes. Section 6 of the CCA provides that if a person who has knowledge of the security measures to access a computer system specifically created by another person illegally discloses such security measures in a manner that is likely to cause damage to another person, such person shall be liable to imprisonment not exceeding one year or to a fine not exceeding THB 20,000, or both.

Section 8 of the CCA provides that a person who illegally makes, by any electronic means, an interception of computer data of another person that is being transmitted in a computer system and such computer data is not for the benefit of the public or is not available for other persons to utilise would be liable to imprisonment not exceeding three years or to a fine not exceeding THB 60,000, or both.

Failure by an organisation to implement cybersecurity measures

Yes. Section 15 of the CCA provides that any service provider who cooperates, consents to or acquiesces in the commission of an offence under Section 14 of the CCA with regards to a computer system in his control would be liable to the same penalty as provided in Section 14 of the CCA.

Section 14 of the CCA provides that whoever commits the following acts shall be liable to imprisonment not exceeding five years or to a fine not exceeding THB 100,000, or both:

(1) dishonestly or deceitfully inputting into a computer system computer data which is distorted or forged, either in whole or in part, or computer data which is false, in such a manner likely to cause injury to the public but not constituting a crime of defamation under the Criminal Code;

(2) inputting into a computer system computer data which is false, in such a manner likely to cause damage to the maintenance of national security, public safety, national economic security, or public infrastructure serving national public interest, or to cause panic amongst the public;

(3) inputting into a computer system computer data which constitutes a crime concerning the security of Thailand or a crime concerning terrorism under the Penal Code;

(4) inputting into a computer system computer data with vulgar characteristics when such computer data is capable of being accessed by the general public; and

(5) publishing or forwarding computer data with the knowledge that it is the computer data under points (1) to (4).

If the acts under (1) to (5) above are not committed against the public but are committed against a particular person, the criminal or the person who publishes or forwards the aforesaid computer data would be liable to imprisonment not exceeding three years or to a fine not exceeding THB 60,000, or both (and the offences are compoundable).

1.2 Do any of the above-mentioned offences have extraterritorial application?

If an offence specified in the CCA is committed outside Thailand and (i) the offender is a Thai national and there is a request for punishment by the government of the country where the offence has occurred or by the injured person, or (ii) the offender is a non-Thai national and the Thai Government or a Thai person is an injured person and there is a request for punishment by the injured person, the offender would be subject to the provisions of the CCA.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Yes. There is an exception which applies only to service providers. In principle, any service provider who cooperates, consents to or acquiesces in the commission of an offence under Section 14 of the CCA with regards to a computer system within his control would be subject to the same penalty as that which is imposed upon a person who commits the offence under Section 14 of the CCA. However, in the case that the service provider is able to prove it has complied with the Ministerial Notification setting out procedures for the notification and suppression of the dissemination of such data and the removal of such data from the computer system, it would be exempt from the penalty (Section 15 of the CCA).

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Yes. Section 269/4 of the Criminal Code provides that whoever uses or acquires for use an electromagnetic record/electronic card which is forged or altered in accordance with Section 269/1 shall be liable to imprisonment of between one and 10 years or to a fine of THB 20,000 to THB 200,000, or both. For example, three men were accused of conspiring to hack and forge electronic card information in the systems of a telecommunications operator to raise the cards' top-up value to THB 105,000,000 and then selling them for THB 12,000,000. They were found guilty of selling forged electronic cards and were imprisoned.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

- The CCA.
- The Electronic Transactions Act 2001.
- The Royal Decree prescribing Criteria and Procedures for Electronic Transactions of the Government Sector 2006.
- The Notifications issued by the Electronic Transactions Commission ("**ETC**").
- The Royal Decree on Security Procedures for Electronic Transaction 2010.
- The Special Case Investigation Act 2004.
- The Telecommunication Business Act 2011.
- Payment Systems Act 2018.
- The National Council for Peace and Order Announcements.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Yes. The ETC's List of Sectors/Organisations that are deemed as Critical Infrastructure and Required to Comply with Strict Security Techniques 2016 impose a list of critical infrastructure organisations which are required to have additional security standards (strict security techniques) in accordance with the Notification of the ETC on Information Security Standards and in accordance with Security Techniques 2012, such as having a teleworking policy, automatic equipment identification, a clean-desk policy, a clear-screen policy and setting up time limits on connections with networks regarded as high risk.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. Commercial banks, e-payment service providers and telecommunications service providers are required by Applicable Laws to take measures to monitor, detect, prevent and mitigate Incidents as per the requirements set out under Applicable Laws (e.g. Bank of Thailand's Notifications and the Notifications of the National Broadcasting and Telecommunications Commission ("**NBTC**"). Please find more details in our answers to question 3.2 below.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

No, there are no conflict of laws issues.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Under the Payment Systems Act, e-payment service providers are required to notify Bank of Thailand ("**BOT**") of an occurrence of any problem or failure to provide e-payment service as soon as possible. E-payment service providers have the obligation to notify BOT of all the problems and failures in relation to their services regardless of whether or not such problem/failure is caused by the occurrence of an Incident. Moreover, e-payment service providers are required to notify BOT within 24 hours if their services are temporarily suspended due to any special circumstances (which may or may not involve an Incident).

With respect to securities companies under the Securities and Exchange Act 1992 ("**SEA**"), securities companies are required to notify, either by verbal or electronic means, the Securities and Exchange Commission ("**SEC**") without delay upon the acknowledgment of a system disruption, unauthorised access to a system or an Incident that results in damage to the security company's reputation, such as website defacement. The notice is required to specify the date and time of the Incident, the type of Incident, the details of the Incident and the effects from the Incident. On the following business day after such acknowledgment, a written report must be submitted to the SEC, which must further specify details of how the Incident is being resolved and the progress made in doing so.

There are no exemptions applicable to e-payment service providers or securities companies in terms of reporting requirements.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Yes. When an Incident occurs, the organisation is entitled to file a report to the police and that report is then handed to the inquiry official to investigate the alleged conduct and file charges against a suspect (if considered appropriate).

There are no legal provisions prohibiting or restricting organisations from notifying foreign authorities or private sector organisations.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The securities companies are required to notify an affected customer or other affected persons without delay upon the acknowledgment of a system disruption, unauthorised access to a system or an Incident that results in damage to the security company's reputation, such as website defacement. There are no specific requirements on the information to be included in the notice given to the affected individuals.

For other sectors, there is no legal requirement to notify Incidents or potential Incidents to any affected individuals.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No. The responses do not change.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

(a) BOT is the regulator of financial institutions and other non-financial institutions as specified by BOT. It is the body responsible for supervising, examining and analysing the performance and risk management systems of e-payment services.

(b) The SEC is the regulator of companies listed on the Stock Exchange of Thailand and is responsible for supervising the standard operating procedures of securities companies, including IT supervision procedures.

(c) A police officer has the authority to initiate an investigation or proceedings relating to a criminal offence, including CCA offences.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

(a) With respect to securities companies under the SEA, the penalty for not complying with the notice requirements under questions 2.5 and 2.7 is a fine not exceeding THB 300,000 and a further fine not exceeding THB 10,000 for every day during which the violation continues. The director, manager or any person responsible for the operation of such securities company shall be liable to imprisonment for a term not exceeding six months or to a fine not exceeding THB 200,000, or both, unless it can be proven that such person has no involvement with the commission of the offence by such securities company.

(b) With respect to e-payment service providers under the supervision of BOT, the penalty for not complying with the notice requirement under question 2.5 is a fine not exceeding THB 1,000,000 or THB 2,000,000 depending on the type of e-payment service providers.

(c) With respect to telecommunications business licensees, they are required to comply with the licensing conditions prescribed in their particular licence, which may include cybersecurity measures. In such case, if a licensee fails to comply with the prescribed licensing conditions, the National Broadcasting and Telecommunications Commission shall have the power to order the licensee to: refrain from carrying out the violating act(s); carry out rectification and improvement; or perform actions correctly or appropriately within a specified period of time. If the licensee fails to comply with the order, the licensee shall be liable to a fine of not less than THB 20,000 per day and in case the licensee still omits to perform the actions correctly, or where there is serious damage to the public interest, the Commission shall have the power to suspend or revoke the licence.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

So far, we have found no non-compliance cases taken by the relevant regulators which have been announced to the public.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes. State agencies have obligations pertaining to specific information security measures, such as the requirement for policies and practices on personal information protection in electronic transactions, IT security practices and policies (which must include provisions relating to access control, user access management, user responsibilities, network control, operating system access control and other provisions as specified by the Office of the Electronic Transactions Commission ("**OETC**")). On the other hand, private sector organisations have fewer legal requirements.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes.

(a) Financial services sector: organisations which operate e-payment services are regulated under the relevant BOT notifications. Principally, e-payment service providers are required to have a contingency plan or a backup system for the purposes of continuity of the service and a safety policy or measures for the information system, which must at least meet the standards prescribed in the BOT notifications. Moreover, e-payment service providers are required to keep customer data confidential throughout and after the use of its services, with certain exceptions. The OETC may also prescribe mandatory practices required to be observed by the e-payment service provider.

(b) Telecommunications sector: the telecommunications sector is administrated by the National Broadcasting and Telecommunications Commission ("**NBTC**"). The NBTC has issued notifications setting out rules and procedures for the management of information technology, and procedures for protecting personal information, rights of privacy and freedom in communication through telecommunications' means. Moreover, the NBTC has the power to prescribe specific provisions concerning cybersecurity to each licensed telecommunications operator.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

There are none in our jurisdiction.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Securities companies are required to conduct cyber risk assessments and vulnerability assessments at least once a year. If a securities company assigns a third party to manage its IT system, the securities company is required to have an Incident response policy. There is no requirement for the appointment of a CISO for securities companies.

These requirements do not apply to private companies.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Securities companies are required to submit an annual report which includes its IT management and occurrence of Incidents to the SEC. E-payment service providers are also required to prepare information and details as to the provision of services and make the same available for inspection by BOT. BOT has the power to instruct an e-payment service provider to provide any information in relation to its services, including information on the occurrence of Incidents.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

The CCA imposes a legal requirement on service providers (e.g. a website service provider) to keep and maintain certain computer data (e.g. IP address, logs) depending upon the characteristics of the service provider. Examples are the requirement to keep relevant computer traffic data in order to be able to identify the user from the beginning of the use of the service and the log showing the use by such user, and store it for not less than 90 days after the end of the service period. The competent official is empowered on a case-by-case basis to order a service provider to maintain such computer traffic data for a period not exceeding two years.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Issues relating to Incidents are governed by the Civil and Commercial Code ("**CCC**") under the section relating to a "wrongful act" (i.e. Section 420 of the CCC). A wrongful act is similar to a tort. Under this provision of law, if any Incident, whether wilfully or negligently, unlawfully damages or injures another person's life, body, health, liberty, property or any right, the party in breach is said to have committed a wrongful act and is bound to pay compensation for damages suffered. The general guidance from the Thailand Supreme Court's decisions is that the injured party is entitled to claim actual damage suffered, with the burden of proof being on the claimant.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

In 2016, the accused was arrested in connection with the attacks that caused some government websites to be blocked and non-public files to be leaked. The legal status of the accused is not yet available to the public.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes. Please see the response to question 5.1 above.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents in our jurisdiction.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

No, there are not any specific requirements under Applicable Law.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No, there are not any Applicable Laws that may prohibit or limit the reporting of the above.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

For the benefit of an investigation, if there is reasonable cause to believe that there is a perpetration of an offence under the CCA, or there is a request by the inquiry official, the competent official is empowered to acquire evidence to prove an offence and to identify the accused, for example, by: (i) issuing an inquiry letter to any person related to the commission of an offence to give statements, forward written explanations or any other documents, data or evidence in a comprehensible form; (ii) requiring computer traffic data related to communications from a service user via a computer system or from other relevant persons; (iii) instructing a service provider to (a) deliver user-related data that is required to be retained under the CCA requirements or that is in the service provider's possession or control to the competent official, or (b) keep the data for later; or (iv) seizing or attaching a computer system for the purposes of obtaining details of the offence and the person who committed the offence.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Yes. As mentioned in question 8.1 above, the competent official has the authority to access a computer system, computer data, computer traffic data or a computer data storage device and to decrypt the computer data of any person, provided that the competent official has obtained a court order to do so.

Saroj Jongsaritwang
R&T Asia (Thailand) Limited
973 President Tower
12th Floor Units 12A – 12F
Ploenchit Road Lumpini Pathumwan
Bangkok 10330
Thailand

Tel: +66 2 656 1991
Email: saroj.jongsaritwang@rajahtann.com
URL: th.rajahtannasia.com

Saroj is a Partner in the Corporate & Commercial Practice of R&T Asia (Thailand) Limited, the Bangkok office of Rajah & Tann LLP. Saroj graduated with a Bachelor of Laws from Thammasat University in 1999, and is a licensed Thai lawyer.

Prior to joining Rajah & Tann, Saroj was a legal counsel (AVP) at a leading Thai consumer finance business, and before that he was in private practice at a local Thai law firm. Saroj has several years' experience in advising on corporate, commercial and consumer finance matters (including personal loans, credit cards and insurance) and agreements relating to the consumer finance business. He regularly advises on employment and TMT matters and is recommended in *The Legal 500* for 2015, 2016, 2017 and 2018 for TMT and Employment, and in *Chambers Asia Pacific* (2017, 2018) in TMT and Banking.

Sui Lin Teoh
R&T Asia (Thailand) Limited
973 President Tower
12th Floor Units 12A – 12F
Ploenchit Road Lumpini Pathumwan
Bangkok 10330
Thailand

Tel: +66 2 656 1991
Email: sui.lin.teoh@rajahtann.com
URL: th.rajahtannasia.com

Sui Lin is the Deputy Managing Partner of R&T Asia (Thailand) Limited, the Bangkok office of Rajah & Tann LLP. Sui Lin graduated with a Bachelor of Laws from the University of London, and is qualified as a solicitor in England & Wales. Before joining Rajah & Tann, Sui Lin was Of Counsel in the dispute resolution group of an international law firm in Thailand. Prior to that, she was a partner in a leading local law firm. She has more than 24 years of experience in Thailand, advising on general corporate and commercial matters, including advising clients in the telecommunications sector and e-commerce businesses on setting up operations in Thailand, and on the handling and use of data under Thai law. She also regularly advises on employment matters and is recommended in *The Legal 500* 2018/19 in this area. Sui Lin is fluent in spoken Thai.

RAJAH & TANN
Thailand

Based in Bangkok, the team in R&T Asia (Thailand) Limited has an impressive base of international, regional and local clients.

We have many years of experience in advising on a range of Thai law matters, including representing clients in civil, criminal or administrative proceedings, international and domestic arbitration, government investigations and compliance proceedings, structuring foreign direct investment and mergers and acquisitions involving private or listed companies, and general corporate commercial matters for foreign investors in Thailand.

The team has particular expertise in representing clients in highly regulated industries, such as telecoms, tobacco, food and beverage, insurance and manufacturing, and can provide full support in large-scale litigation, transactions and investigations.

The team comprises a majority of Thai nationals who are qualified to advise on Thai law. Our Thai lawyers are fluent in Thai and English and are fully conversant with the practical application of the law within Thailand's business and cultural landscapes.

Tunisia

Amina Larbi

Ferchiou & Associés

Rym Ferchiou

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes.

The act of fraudulent access to or hindering all or part of an automated data processing system is a criminal offence sanctioned by article 199 *bis* (1) of the Tunisian Criminal Code ("**TCC**").

Maximum penalties: two months to one year of imprisonment and/or a 1,000 Tunisian Dinar ("**TND**") fine.

It is increased to two years of imprisonment and a 2,000 TND fine when the hacking results in an alteration or destruction of the functioning of existing data in that system, even without fraudulent intent.

Denial-of-service attacks

Causing an interruption of telecommunications by the breaking of lines or the deterioration or destruction of equipment by any means whatsoever is an offence as per article 82 of the Code of Telecommunications.

Denial-of-service attacks could also be interpreted as an offence under article 199 *bis* (3) TCC relating to intentionally altering or destroying the operation of automated processing.

Maximum penalties: five years of imprisonment and/or a 20,000 TND fine for deteriorating or destroying telecommunication equipment by any means, or three years of imprisonment and a 3,000 TND fine for intentionally altering or destroying the operation of an automated process.

Phishing

Yes.

Considering that phishing aims to induce individuals to reveal personal information, this would be considered as illegal collecting and processing of personal data, which would be sanctioned by articles 88 and 94 of Law n° 2004-63 dated 27 July 2004 regarding the protection of personal data (the "Personal Data Protection Law").

Maximum penalties: one year of imprisonment and a fine of 10,000 TND for using fraud to obtain and or process personal data, or eight months of imprisonment and a fine of 1,000 TND for collecting personal data for illegitimate aims.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. The act of introducing data into an automated processing system that may alter the data contained in the program or its method of processing or transmission is an offence falling under article 199 *bis* (4) TCC.

Maximum penalties: three years of imprisonment and a 3,000 TND fine for intentionally altering or destroying the operation of an automated process, or 10 years of imprisonment and a fine of 5,000 TND if the offence is committed while performing professional duties (i.e., by an employee performing his work).

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

There is no explicit text sanctioning such possession *per se*.

However, if the possession is made in bad faith to cover cybercrime activities, the possessor may be considered an accomplice of the offender and incurs criminal sanctions.

Concerning the use of hardware, software or other tools used to commit cybercrime, considering that cybercrimes constitute offences and that attempts are punishable, any tool used to commit cybercrime can be considered as proof of the intent to commit such crimes that would trigger sanctions.

The sanctions depend on the nature of the cybercrime committed.

Identity theft or identity fraud (e.g. in connection with access devices)

Yes.

Under article 261 TCC, theft is defined as the fact of fraudulently subtracting anything.

Electronic theft of data would be considered theft under Tunisian law and sanctioned with five years of imprisonment and 120 TND fine.

Electronic theft could also be interpreted as an offence, falling under article 199 *bis* (1) TCC with the same sanctions provided under "Hacking" above, or as an offence falling under the Personal Data Protection Law.

See "Hacking" and "Phishing" above.

Also, this offence could fall under the illegal use of personal encryption elements relating to the signature of third parties (which is a form of identity theft) based on article 48 of Law n° 2000-83, dated 9 August 2000, regarding electronic commerce. It is sanctioned with imprisonment for up to two years and/or a fine of up to 10,000 TND.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Yes.

Under article 261 TCC, theft is defined as the fact of fraudulently subtracting anything.

Electronic theft of data would be considered theft under Tunisian law and sanctioned with five years of imprisonment and a 120 TND fine.

Electronic theft could also be interpreted as an offence falling under article 199 *bis* (1) TCC with the same sanctions provided under "Hacking" above.

More specifically, electronic theft of funds is an offence as per Law n° 2005-51 dated 27 June 2005 relating to electronic transfer of funds ("Electronic Transfer of Funds Law"). Indeed, the use of a falsified transfer instrument is heavily sanctioned.

As per Law n° 94-36 dated 24 February 1994 on literary and artistic property ("Copyright Law"), the use of any protected work under copyright without obtaining proper authorisation is sanctioned. The misuse could be the result of an electronic theft.

Maximum penalties: 10 years of imprisonment and a 10,000 TND fine for use of falsified transfer instruments (Article 17 of the Electronic Transfer of Funds Law).

Maximum penalties: a fine of one up to 1,000,000 TND and/or imprisonment of up to 12 months in case of a recurrence of the copyright offence (Article 52 of the Copyright Law).

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Introducing a modification of any kind to the content of an original electronic document, provided that it causes damages to third parties, is sanctioned with two years of imprisonment and a 2,000 TND fine as per article 199 *ter* TCC.

The attempt to do so is also sanctionable.

In addition, the Telecommunication Code imposes a fine ranging from 1,000 TND to 5,000 TND on any person who destroys or deteriorates by any means whatsoever telecommunication (transmission) lines or equipment.

Under the same code, the voluntary causing of telecommunication disruption through the breaking of lines, and the destruction or the deteriorating of telecommunication equipment is punishable by six months to five years of imprisonment and/or a fine ranging from 1,000 TND to 2,000 TND.

Also, the hijacking of telecommunication lines is punishable with five years of imprisonment.

Moreover, the disclosure, incitement or participation in the disclosure of telecommunication contents and exchanges transmitted through telecommunication networks are punishable with three months of imprisonment.

The voluntary disturbance of other people's peace through public network telecommunication is punishable with one to two years of imprisonment and a fine ranging from 100 TND to 1,000 TND.

Failure by an organisation to implement cybersecurity measures

Yes.

Law n° 2004-5 dated 3 February 2004 relating to electronic security ("Electronic Security Law") and Decree n° 2004-1250 impose that public entities, companies that are operators of public telecommunications networks and providers of telecommunications and internet services, companies whose computer networks are interconnected through external telecommunications networks, and companies performing automated processing of their customers' personal data in connection with the provision of their services through telecommunications networks must perform a mandatory audit to check their computer systems and networks at least once every 12 months. If they fail to meet this obligation, the Network and Information Security Agency ("**NISA**") will notify the entity to perform such audit, otherwise the audit will be conducted by the NISA by a certified NISA expert. The expenses will be borne by the breaching entity (articles 5 and 6 of the Electronic Security Law and article 8 of Decree n° 2004-1250).

Also, private and public entities must implement the measures ordered by the NISA in order to preserve the safety of the networks in case of any cyber-attack, and they can also face a shutdown to protect the entire national network (articles 10 and 11 of the Electronic Security Law).

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, in the absence of specific provisions relating to the extraterritorial effect of applicable laws in relation to cybersecurity offences, we would refer to criminal common principles, whereby, pursuant to article 305 of the Code of Criminal Procedures ("CCP"), it is possible to prosecute a Tunisian citizen (for a crime or an offence committed outside the Tunisian territory) unless the foreign country's laws do not prohibit such acts, or the accused has been tried abroad, and in case of conviction, he completed his sentence.

In addition, as per article 307 of the CCP, it is possible to prosecute a foreigner in Tunisia who has committed a crime or an offence against State security (i.e., national security) if he/she get arrested in Tunisia or the Government obtains his/her extradition.

Also, any person who is accused of committing a crime or an offence outside the Tunisian territory against a Tunisian citizen may be prosecuted and tried before courts in Tunisia.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Without prejudice to the rights of victims, the Minister in charge of Communication Technologies can issue request for settlement for offences relating to the deterioration or destruction of telecommunication equipment that were not intentionally committed. Payment of the sum fixed by the settlement agreement, if any, extinguishes the public action and prosecution of the administration.

In specific cases relating to terrorism attacks, the offender can obtain an exemption or a reduction of the incurred punishment further to providing information to the competent authority of an offence to be committed (article 8 and 9 of the Anti-Money Laundering and Anti-Terrorism Law n° 2015-26 of 7 August 2015 – "Anti-Money Laundering and Anti-Terrorism Law").

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Yes, as per article 14 (7) of the Anti-Money Laundering and Anti-Terrorism Law n° 2015-26 of 7 August 2015, damaging a computer system in the frame of a terrorist attack is punished with a maximum of a life sentence if the offence resulted in bodily injuries.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

a) Binding regulations

- The Tunisian Criminal Code.
- The Telecommunications Code.
- Law n° 2004-5 dated 3 February 2004 relating to electronic security and on the organisation of the field of computer security and setting the general rules for the protection of computer systems and networks (the Electronic Security Law).
- Decree n° 2004-1250 dated 25 May 2004 fixing the computer systems and networks of organisations subject to the periodic compulsory audit of IT security and the criteria relating to the nature of the audit and its periodicity and the procedures for follow-up on the implementation of the recommendations contained in the audit report.
- Circular n° 19 dated 11 April 2007 regarding reinforcement of cybersecurity measures in public institutions.
- Circular n° 19 dated 18 July 2003 on safety and prevention measures for the buildings of ministries and local authorities and public enterprises.
- Law n° 2000-83 dated 9 August 2000 regarding electronic commerce (the "**Electronic Commerce Law**").
- Decree n° 2008-2639 dated 7 July 2008 setting the conditions and procedures for importing and marketing encryption tools or services through telecommunications networks.
- Law N° 2005-51 dated 27 June 2005 relating to electronic transfer of funds (the Electronic Transfer of Funds Law).
- Law n° 2004-63 dated 27 July 2004 regarding the protection of personal data (the Personal Data Protection Law).
- Law n° 94-36 dated 24 February 1994 on literary and artistic property (the Copyright Law).
- Law n° 2015-26 dated 7 August 2015 regarding anti-terrorism and anti-money laundering (the Anti-Money Laundering and Anti-Terrorism Law).

b) Non-binding regulatory guidance for professional users

- NISA Internet Policy Guidance.
- NISA Charter of Good Use of Computer Systems.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The concept of critical infrastructure is not embodied under the Applicable Laws. However, we assume that such infrastructures are those that treat or contain sensitive data relating to national security and interest, owned by Government or State entities such as the Ministry of Interior Affairs and the Ministry of National Defence – which are excluded from the cybersecurity requirements including the compulsory audit requirement. Specific procedures must be set in coordination with the Ministry of National Defence and the Ministry of Interior Affairs and Local Development.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes.

Specific entities must perform a mandatory audit to check their computer systems and networks at least once every 12 months to detect and prevent Incidents.

Also, private and public entities must implement the measures ordered by the NISA upon receiving information by this authority of any Incident in order to preserve the safety of the networks in case of any cyber-attack. The Ministry in charge of Communication Technologies can issue a decision (based on a NISA proposal) to isolate the relevant network to protect the entire national network.

Per Circular n° 19 dated 11 April 2007, public enterprises are expected to prevent Incidents through the creation of a "Computer Security Cell" in order to coordinate with the NISA and a "Computer Security Committee".

Also, per the guidance of the NISA, private entities shall implement a certified information security management system ("**SMSI**" in French) for the safe use of computer systems and networks.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

No. We do not believe that such requirement would interfere or conflict with other laws.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes.

a) In the event of an attack, intrusion or disruption that is likely to impede the operation of another computer system or network (article 10 of the Electronic Security Law).

b) A public or private entity is required to inform the NISA.

c) No limited scope is provided. We assume that such report should include information on the nature of the attack, intrusion or disruption.

d) No exceptions exist. At the same time, no stipulation in the Electronic Security Law provides that such reporting to the NISA shall be made public.

However, this does not exclude that local authorities may require, for national security or defence reasons, such information to remain confidential (non-public).

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

The only regulatory authority that must be informed of Incidents is the NISA.

After satisfying the reporting obligation to the NISA, there should be no prohibition to voluntarily share information relating to an Incident with other authorities outside Tunisia, or with any other entities.

Please note that Tunisia has been invited to sign the Budapest Treaty regarding cybersecurity, thus other extraterritorial authorities may have to be informed in the future.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

There is no specific duty under Applicable Laws that would require organisations to report information related to Incidents or potential Incidents to any affected individuals.

However, from a civil liability perspective, it is recommended to inform individuals of Incidents or potential Incidents that may have an adverse effect. This could mitigate the organisations' responsibility and the impact of such Incident on concerned individuals.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Considering that the information set in the question includes personal data, although Applicable Laws do not specifically apply, we assume that informing the Data Protection Authority and the individual concerned would be strongly expected.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Network and Information Security Agency (NISA) was created by the Electronic Security Law. NISA is a public enterprise practising its activity under the supervision of the Ministry in charge of Communication Technologies (https://www.ansi.tn/index.html).

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The Applicable Laws do not provide for specific sanctions except what was raised under question 1.1, "Failure by an organisation to implement cybersecurity measures", above (i.e. an audit conducted by the NISA with the expenses borne by the breaching entity).

However, directors may be held liable under tort liability principles for breach of the provisions of the law if such breach results in prejudice suffered by any third parties.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

No specific examples are publicly available.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes.

Based on the Electronic Security Law and Decree n° 2004-1250, additional requirements are imposed upon public entities, companies that are operators of public telecommunications networks and providers of telecommunications and internet services, companies whose computer networks are interconnected through external telecommunications networks, and companies performing automated processing of their customers' personal data in connection with the provision of their services through telecommunications networks.

According to NISA statistics, financial institutions in the private sector were audited heavily between 2010 and 2016 (https://www.ansi.tn/fr/pages/statistics/years/audit.html).

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes. Please see question 3.1.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Tunisian law does not provide for a specific sanction applicable to a company that failed to comply with the provisions of cyber-criminality laws, except what was raised under question 1.1, "Failure by an organisation to implement cybersecurity measures", above (i.e. an audit conducted by the NISA with the expenses borne by the breaching entity).

However, directors may be held liable for breach of the provisions of the law if such breach adversely affected third parties.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

a) Yes, companies mentioned under Decree n° 2004-1250 are required to designate a chief information security officer (CISO) (Circular n° 19 of 11 April 2007 regarding reinforcement of cybersecurity measures in public institutions).

b) Yes, the companies referred to above must establish a written Incident response plan and update it annually.

c) Yes. Conducting periodic cyber risk assessments is mandatory for the above-mentioned entities (see question 1.1, "Failure by an organisation to implement cybersecurity measures" and question 2.3). However, there are no legal requirements to include third-party vendors within the cyber risk assessment.

d) Yes, during audits (article 3 of Decree n° 2004-1250).

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No, except for the requirements mentioned in question 2.3.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, there are no specific requirements in this regard.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The civil action that may be brought is a tort action (for damages under extra-contractual liability).

Per articles 82 and 83 of the Code of Obligations and Contracts, there are three elements to be evidenced:

1) the fault (either intentional or non-intentional);

2) the damage suffered; and

3) the link between the fault and damage suffered.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

To the best of our knowledge, there is no published caselaw related to Incidents.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes. Please see question 5.1.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, per article 4 of the Insurance Code, every legitimate interest can be insured.

Such Incidents are not commonly insured as they correspond to new risks in Tunisia. However, few insurance companies have started to offer insurance coverage for similar risks.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, parties can freely agree on any conditions provided that it does not contravene public order rules and good morals.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

a) Yes, per the NISA Internet Policy Guidance, a set of rules is provided to monitor employees in this regard.

b) Yes, per the NISA Charter of Good Use of Computer Systems, each user is required to report every anomaly to the administrator.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No, there are no Applicable Laws that prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Per the Criminal Procedures Code, judicial police officers may be relied upon to investigate an Incident. In practice, they have broad powers (hearings, testimony and evidence collection, etc.).

Judicial police officers are the following: public prosecutors; cantonal judges; police officers; officers of the national guard; the "Sheikhs"; authorised administrative agents; and investigating judges.

Infringements of the provisions of the Telecommunication Code are mainly investigated by the judicial police officers referred to above, sworn agents of the Ministry in charge of Communication Technologies and the Ministry of Interior Affairs, etc.

Under anti-terrorism law, judges of the anti-terrorism division are the competent body to investigate a terrorist incident; to do so, several means are offered to them: they can intercept calls; perform undercover infiltration; and conduct audio-visual surveillance.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Yes.

Under the Applicable Laws, there are no special obligations for organisations to implement backdoors. However, according to article 14 of Decree n° 2008-2639 dated 7 July 2008, if these organisations are ordered by special services of the Ministry of Defence or the Ministry of Interior Affairs to provide any type of information regarding encryption tools, including encryption keys, they must answer this request without delay.

Amina Larbi
Ferchiou & Associés
34, Place du 14 janvier 2011
1001 Tunis
Tunisia

Tel: +216 71 120 500
Fax: +216 71 350 028
Email: a.larbi@falaw.tn
URL: www.ferchioulaw.com

Amina Larbi is a Partner at Ferchiou Associés and a Member of the Paris Bar (1993) & Tunis Bar (2014).

Education

1993: Certificate in private international law, Den Haag Academy of International Law.

1992: Postgraduate degree (DEA) in private international law and international trade law, University of Paris I, Panthéon Sorbonne.

Experience

With more than 20 years of experience, almost half of them with internationally reputable firms in Paris, Amina has developed a strong expertise in a range of business law areas including foreign investments, M&A, economic law, project set-up and financing (including PPPs), telecommunications PPPs, retail business support and real estate and urbanistic projects.

Rym Ferchiou
Ferchiou & Associés
34, Place du 14 janvier 2011
1001 Tunis
Tunisia

Tel: +216 71 120 500
Fax: +216 71 350 028
Email: r.ferchiou@falaw.tn
URL: www.ferchioulaw.com

Rym Ferchiou is a Junior Partner at Ferchiou & Associés and a Member of the Tunis Bar (2015).

Education

2010–2012: Master 2 Fiscal Law – thesis on intergroup transactions – with high honours (Faculty of Legal, Political and Social Sciences of Tunis).

2009–2010: Master 1 Business Law (University of Paris 1, Panthéon-Sorbonne).

Experience

Rym focuses on all aspects of business law, especially M&A and general corporate matters.

She also assists clients with their investments in Tunisia, including all foreign exchange aspects.

Rym has gained significant experience in other areas such as banking and finance, tax, the stock exchange and competition law.

USA

Keren Livneh

Jacob Reed

Allen & Overy LLP

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Yes; **hacking** (i.e., unauthorised access), **denial-of-service attacks** (DDoS attacks), **phishing**, **infection of IT systems with malware** (including ransomware, spyware, and viruses), **possession or use of hardware**, **software or other tools used to commit cybercrime** (e.g., hacking tools), **identity theft or identity fraud** (e.g., in connection with access devices), and **electronic theft** (e.g., breach of confidence by a current or former employee, or criminal copyright infringement) may constitute criminal offences in the United States.

Computer crimes are principally prosecuted under the Computer Fraud and Abuse Act (CFAA). The CFAA criminalises **hacking**, **DDoS attacks**, **malware**, **identity theft**, and **electronic theft**. Violators may face up to 20 years in prison, restitution, criminal forfeiture, and/or a fine. In addition, in certain circumstances, the CFAA allows the victims of computer crimes to bring private civil actions against violators for compensatory damages and injunctive or other equitable relief.

Additional crimes defined in Title 18 of the United States Code that may be committed through a breach of cybersecurity are:

- Sections 1028 and 1028A criminalise **identity theft** and aggravated identity theft. Violators may face up to 15 years in prison, restitution, criminal forfeiture, and/or a fine.
- Section 1029 criminalises access device fraud and has been used to prosecute **phishing** and **identity theft**. Violators may face up to 20 years in prison, restitution, criminal forfeiture, and/or a fine.
- Section 2701 (also known as the Stored Communications Act) criminalises unlawful access to stored communications, including **electronic theft**. Violators may face up to one year in prison, restitution, criminal forfeiture, and/or a fine.

In recent years, there have been several high-profile "hacking and trading" prosecutions that demonstrate how various criminal statutes interact in relation to computer crimes. For example, in August 2015, the U.S. Department of Justice charged nine people in an international scheme to hack business newswire companies to steal non-public financial information that the individuals used to make stock trades that generated $30 million in illegal profits. The charges included wire fraud, securities fraud, money laundering, computer fraud, and aggravated identity theft.

Similarly, in November 2017, the U.S. Department of Justice charged a day trader who conspired to hack into victims' online brokerage accounts and used them to liquidate positions and place unlawful trades. The charges included conspiracy to commit securities fraud and computer intrusions, conspiracy to commit wire fraud, and conspiracy to commit money laundering.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

In addition to the statutes identified above, the U.S. criminal code includes statutes that criminalise activity that adversely affects or threatens the security, confidentiality, integrity or availability of IT systems, infrastructure, communications networks, devices or data.

For example, the Wiretap Act criminalises the unauthorised interception of a communication or the subsequent disclosure or use of an intercepted communication, as well as the manufacture, distribution, or possession of equipment to be used for unlawful interception. Violators may face up to five years in prison, a fine and, in certain circumstances, civil damages.

In addition, the CAN-SPAM Act creates several computer crimes involving spam email, including accessing a computer without authorisation to send spam email, falsely registering for email accounts or domain names to send spam, materially falsifying email header information, and hiding the origin of spam email. Violators may face up to three years in prison and fines of over $40,000 for each email sent in violation of the statute.

Failure by an organisation to implement cybersecurity measures

No federal statutes universally criminalise an organisation's failure to implement cybersecurity measures. There are, however, sector-specific data protection regulations that may result in regulatory enforcement action, including potential fines and/or exposure to damages in a civil action (e.g., the Gramm-Leach-Bliley Act discussed in section 3.2(a) below and the Health Insurance Portability and Accountability Act). In addition, the Federal Trade Commission may assess penalties against organisations that fail to take reasonable cybersecurity precautions to protect consumer data.

In addition, many states have laws or regulations that impose cybersecurity, data protection, or notification requirements on covered organisations. For example, in 2017, New York's Department of Financial Services implemented its Cybersecurity Regulation, which requires banks, insurance companies, and other covered entities to establish and maintain a cybersecurity programme designed to protect consumers and ensure the safety and soundness of New York State's financial services industry. Similarly, in 2018 the state of Colorado enacted privacy and cybersecurity legislation that will require covered entities to implement and maintain reasonable procedures around the protection and maintenance of confidential information.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Several of the statutes that create the above-mentioned offences provide explicitly for extraterritorial jurisdiction. Even in the absence of an explicit provision for extraterritorial jurisdiction, however, U.S. prosecutors often take a broad view of the statutes' jurisdictional reach and will likely assert jurisdiction over computer crimes that were intended to cause or actually caused detrimental effects within the United States, including any damage or illicit access to systems or servers in the U.S.

Similarly, state laws or regulations may apply to entities that are licensed or regulated in a particular state regardless of where those entities are headquartered, and state prosecutors may assert jurisdiction over any such entities that have violated state laws or regulations.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

A number of factors, including cooperation with investigators, use of outside counsel and experts to conduct a thorough internal investigation, and remediation efforts, are relevant to the determination of criminal and civil penalties imposed by government regulators in enforcement proceedings. As discussed in question 7.2 below, disclosure of information by "whistleblowers" is also protected under a number of statutes.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

In appropriate circumstances, U.S. prosecutors may prosecute computer crimes under other criminal statutes, even if the conduct might also be prosecuted as computer crimes. For example, prosecutors may proceed under piracy, intellectual property, harassment, espionage, or securities fraud statutes, because those statutes have more generous statutes of limitation, provide greater investigative authority, or authorise higher penalties. As noted in question 1.1 above, charges for wire fraud, securities fraud, money laundering, computer fraud, and aggravated identity theft have been brought against hackers who traded on the non-public information they obtained.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

In the United States, numerous federal and state laws and regulations govern cybersecurity issues, with the applicability of particular regulations depending on the sector and geographic operations of the organisations in question.

There is no overarching federal **data protection or Incident management** law, but federal law does prescribe requirements for healthcare providers (in the Health Insurance Portability and Accountability Act (HIPAA)) and the financial services and telecommunications sectors (as discussed in section 3 of this chapter). By contrast, every state has now enacted laws requiring notification of affected individuals and/or state regulators following cybersecurity Incidents, and many states also have information security statutes. For example, Massachusetts's Standards for the Protection of Personal Information of the Residents of the Commonwealth imposes regulations to safeguard the personal information of state residents. Some states also have sector-specific statutes, such as New York's Cybersecurity Regulation, applicable to banks, insurance companies, and other covered entities.

The Electronic Communications Privacy Act (ECPA) establishes **privacy** protection for data and electronic communications in transit or in storage and prohibits warrantless pen register and trap and trace operations involving electronic communications.

The United States maintains a comprehensive **export control** regime that is governed by the Arms Export Control Act (AECA), the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), and the Commerce Control List (CCL). These laws impose export controls on cryptographic and other cybersecurity-related technology. Additionally, the United States is party to the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, which was amended in 2013 to cover export controls on "intrusion software" and "IP network communications surveillance systems". After substantial pressure from private industry and the security research community, in December 2017 the U.S. negotiated a number of amendments to specifically exempt vulnerability disclosure and cyber Incident response activities from these export controls, as well as software used to research intrusion software.

In addition to the Applicable Laws described above, criminal laws in the United States address various computer crimes. Applicable cybersecurity-related criminal statutes are discussed in section 1 of this chapter.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Under the USA PATRIOT Act, 16 sectors (including communications, critical manufacturing, defence industrial base, nuclear reactors, and transportation systems) have been designated as comprising critical infrastructure as to which the federal government must enhance cybersecurity and deepen engagement with private sector actors.

Executive Order 13636 (Improving Critical Infrastructure Cybersecurity), Presidential Policy Directive/PPD-21 (Critical Infrastructure Security and Resilience), and Executive Order 13800 (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure) direct the federal agencies that oversee the designated sectors to develop cybersecurity risk management rules. To varying degrees, the Departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security, Transportation, and Treasury have promulgated sector-specific requirements and recommendations, and have established sector-specific programmes that involve relevant private parties and state governments.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes, federal law requires organisations in certain sectors to take measures to monitor, detect, prevent or mitigate Incidents. Several federal regulatory agencies, notably the U.S. Securities and Exchange Commission, have indicated that they will monitor regulated entities' cybersecurity risk management systems and controls, and require public disclosure relating thereto. In 2017, the SEC announced the creation of a Cyber Unit within its Enforcement Division to specifically focus on cyber-related misconduct. In February 2018, the SEC also released an Interpretive Statement and Guidance on Public Company Cybersecurity Disclosures, which expanded previous guidance and stressed that regulated companies have an affirmative obligation to disclose material cybersecurity risks and Incidents and that an ongoing Incident investigation does not allow a company to avoid making such disclosures. And in April 2018, the SEC charged Altaba Inc. (formerly Yahoo! Inc.) with failing to disclose a material cybersecurity breach. Altaba agreed to pay a $35 million civil penalty to settle the SEC's charges.

As noted in question 2.1, all 50 states have now implemented laws applying Incident-related requirements on organisations.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Federal cybersecurity regulations are largely consistent, though organisations that operate in multiple regulated sectors could encounter conflicting requirements or expectations.

The greatest risk of conflict of laws issues exists with respect to state law systems, which may vary greatly. For example, all states have independent data breach notification requirements, which require covered organisations to provide notifications to particular individuals or entities, in particular formats, and within specified time periods. State law requirements on those points may be inconsistent. Differing notification requirements create a significant compliance challenge for companies operating in multiple jurisdictions.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes. Applicable Laws include a number of sector-specific Incident notification requirements. For example, HIPAA imposes notification requirements on healthcare providers who suffer data breach Incidents. Under HIPAA, in the event of a data breach, covered entities must notify the Secretary of Health and Human Services. The timing of the notification depends on the number of individuals whose protected health information was compromised. Covered entities are not required to include data like malware signatures or other technical information, though investigators may seek access to this information if the Incident becomes the source of a criminal investigation. Because HIPAA only requires notification for breaches of protected health information, certain healthcare providers have not provided notification for other Incidents, such as ransomware attacks.

As noted in question 2.3, in 2018 the U.S. Securities and Exchange Commission released updated guidance on cybersecurity disclosures, stating that any publicly traded or SEC-regulated company is expected to report material data breaches.

In addition, all states have their own Incident notification laws. For example, New York's Cybersecurity Regulation requires covered financial entities to provide notice to the Superintendent of New York's Department of Financial Services within 72 hours after certain cybersecurity events.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Yes, the Cybersecurity Information Sharing Act (CISA) authorises private entities to voluntarily share cyber threat indicators or defensive measures with certain government or quasi-government entities (including federal, state, and local governments and regulatory authorities).

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

In certain sectors governed by federal law and under many state laws, organisations are required to notify affected individuals that their information has been compromised. The content and timing of the required notifications varies.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The sharing of such information with regulators or other law enforcement authorities is explicitly authorised by the CISA. In addition, items (b) through (d) are unlikely to be protected information under U.S. law and may be disclosed more broadly.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The enforcement of federal Incident-related laws varies by sector. For example, the Office for Civil Rights at the Department of Health

and Human Services investigates violations of HIPAA's cybersecurity requirements, the SEC investigates federal securities laws relating to cybersecurity, the Federal Trade Commission (FTC) investigates compromise of consumer information through cybersecurity breaches, and the Department of Justice prosecutes violations of federal criminal cybersecurity statutes.

Most states have similar sector-specific enforcement frameworks. For example, the Superintendent of the New York Department of Financial Services is responsible for enforcing the Cybersecurity Regulation. Other states may grant enforcement authority to the Attorney General or agencies responsible for consumer protection.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

There is no overarching penalties framework for violations of federal laws. Rather, penalties vary depending on the particular laws, rules or regulations at issue. For example, HIPAA imposes maximum fines up to $50,000 per violation and $1.5 million per organisation per calendar year. Additionally, the U.S. Federal Sentencing Guidelines will be used in determining the criminal sanctions for individuals who face federal prosecution for any criminal actions leading up to or in response to Incidents.

Similarly, there is no overarching penalties framework for violations of state laws and possible penalties may vary greatly from state to state. Some states' penalties frameworks are based on consumer protection laws or specific cybersecurity statutes; some states' cybersecurity laws, including New York's Cybersecurity Regulation, are silent on penalties.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The failure of companies to implement adequate cybersecurity programmes to protect against and mitigate Incidents has resulted in enforcement action across numerous sectors. For example, in 2018, Altaba Inc. (formerly Yahoo! Inc.) agreed to pay the SEC a $35 million penalty to settle charges for failing to disclose its 2014 data breach, which was the largest known theft of user data at the time, and for making materially misleading statements in its quarterly and annual reports for the next two years. In 2016, the Canadian company Ashley Madison settled FTC and state charges for its 2015 customer data breach, ultimately paying $1.6 million. In 2015, Wyndham Hotels settled FTC charges for failing to prevent or mitigate multiple data breaches. The settlement established a 20-year compliance programme for Wyndham, requiring them to implement a security programme and receive regular audits and assessments.

Between 2003–2018, the HHS Office of Civil Rights has settled or imposed penalties in 55 cases against organisations alleged to have violated HIPAA data security requirements, resulting in almost $79 million in aggregate penalties.

In June 2018, Equifax agreed to a consent order with an eight-state team of regulatory agencies, including New York and California, which required certain changes to Equifax's IT management, risk mitigation and management oversight in response to the 2017 Equifax data breach, which resulted in the theft of personal information of over 145 million people.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, market practice with respect to information security varies significantly across industry sectors. Organisations in well-regulated industries like the financial services sector are more likely to have established cybersecurity processes in accordance with the relevant regulations (e.g., SEC-regulated firms must have written policies to protect customer information under SEC Regulation S-P). Financial services firms also recognise the financial risk of customer financial information being released – a 2017 FINRA report revealed that most broker-dealer firms that FINRA examined had significantly increased their focus on cybersecurity risks in the previous two years and had established, or were establishing, cybersecurity risk management practices. Other industries that perhaps have fewer cybersecurity regulations or face competing priorities are less likely to have established robust cybersecurity practices. For example, the retail industry – where narrow profit margins might discourage the deployment of expensive defensive software or equipment – only recently began investing significant resources into cybersecurity after a number of high-profile data breaches.

In addition to the differences in market practice across sectors, market practices can differ greatly within a specific sector based on the size and sophistication of individual entities. For example, even though the healthcare industry must protect customer information under the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA), the rule is flexible and allows smaller healthcare providers to incorporate less advanced cybersecurity practices based on their capability, technical infrastructure, and ability to cover the cost of a solution. In fragmented industries like healthcare, market practice will vary significantly and many smaller entities will be less capable of preventing, detecting, mitigating or responding to cybersecurity Incidents.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

(a) Financial Services Sector

Federal laws, as well as regulatory agency rules or regulations, impose data protection and cybersecurity requirements on organisations in the financial services sector. Examples include:

- The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to "establish appropriate standards" to safeguard customer information and imposes fines of up to $100,000 for institutions and $10,000 for individual officers for each violation.
- The Safeguards Rule (also known as SEC Regulation S-P) requires regulated firms to adopt and implement written policies and procedures to protect customer information.
- The Federal Deposit Insurance Act (FDIA) imposes "operational and management standards", which include "internal controls, information systems, and internal audit systems".

- The Interagency Guidelines Establishing Information Security Standards set forth information security standards under the FDIA and require financial institutions to maintain an information security programme to safeguard the confidentiality and security of customer information and ensure the proper disposal of customer information.
- The Fair and Accurate Credit Transactions Act (FACTA) requires the proper disposal of customer information.
- The Red Flags Rule (also known as the Identity Theft Rule or SEC Regulation S-ID) imposes on regulated firms a duty to detect, prevent and mitigate identity theft.
- The Securities Exchange Act of 1934 requires firms to preserve electronically-stored records in a non-rewritable, non-erasable format.

State laws, rules or regulations may also impose data protection and cybersecurity requirements on organisations in the financial services sector. Importantly, New York's Cybersecurity Regulation requires covered entities to establish and maintain a cybersecurity programme designed to protect consumers and ensure the safety and soundness of New York State's financial services industry. In response to the 2017 Equifax data breach, New York expanded its Cybersecurity Regulation to include credit reporting agencies with significant operations in New York, which are now obligated to comply with the regulation starting in November 2018.

(b) Telecommunications Sector

The Communications Act requires telecommunications carriers to take steps to ensure that customer proprietary network information (CPNI) is protected from unauthorised disclosure. To that end, the Communications Act directs covered entities to follow FCC standards for protecting CPNI.

Additionally, state laws, rules or regulations in relation to cybersecurity requirements may apply to, or have specific requirements for, the telecommunications sector.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

The failure to implement and maintain an adequate cybersecurity programme might expose directors and officers to liability in shareholder derivative lawsuits. Directors and officers owe fiduciary duties to their shareholders that include overseeing enterprise risk management. Directors and officers who are not meaningfully involved in overseeing the risk management of the company, or who are negligent in their response to cyber Incidents, may face liability.

The 2013 Target Corp data breach is a noteworthy example. In the ensuing lawsuit, the plaintiffs argued that Target Corp's directors failed to adequately manage the risk of a cybersecurity Incident both before and after the data breach. Following a two-year special litigation committee investigation, the derivative action against Target Corp and its directors was dismissed because the company and its directors made consistent, deliberate efforts to address cybersecurity requirements and risks.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The Safeguards Rule (SEC Regulation S-P) requires financial institutions, broker-dealers, and investment firms to designate one or more employees to coordinate its information security programme. In addition, the New York Cybersecurity Regulation requires covered entities to **designate a CISO**.

The Interagency Guidelines Establishing Information Security Standards direct covered entities to include **Incident response programmes** in their information security programmes. In addition, the SEC and the Financial Industry Regulatory Authority (FINRA) have stated that their examination programmes will test the implementation of cybersecurity procedures and controls by investment advisors and broker-dealers. The New York Cybersecurity Regulation requires covered entities to have a written Incident response plan. Other states' laws may require Incident response plans for certain organisations that operate in their jurisdiction.

The Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice directs financial institutions to conduct **risk assessments** as part of their information security programmes. The guidance also directs institutions to address Incidents in systems maintained by third-party service providers. In addition, the New York Cybersecurity Regulation requires covered entities to conduct regular risk and vulnerability assessments, including risk assessments of third-party service providers. Other states' laws may require risk assessments by organisations that operate in their jurisdiction.

The Interagency Guidelines Establishing Information Security Standards direct covered entities to regularly **test information security controls, systems and procedures**. The guidelines recommend that the tests be performed, or reviewed, by independent third parties. The New York Cybersecurity Regulation requires covered entities to perform annual penetration testing and bi-annual vulnerability assessments. Other states' laws may require penetration testing or vulnerability assessments by organisations that operate in their jurisdiction.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Federal law establishes breach notification only for specific sectors, such as healthcare facilities, which are required under HIPAA to notify affected individuals through various media following a breach. As noted in question 2.3, in 2018 the U.S. Securities and Exchange Commission released guidance that all publicly traded or SEC-regulated companies are expected to report material data breaches.

Separately, all 50 states have passed laws requiring organisations to notify affected individuals of security breaches in which personal information was compromised. While state law notice requirements differ, many require individual notifications to affected individuals, as well as notifications to state authorities or consumer reporting agencies. For example, New York's Cybersecurity Regulation requires notice to the Department of Financial Services Superintendent following cybersecurity events that impact covered entities.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

This chapter outlines the principal federal laws and requirements relating to cybersecurity. State laws and regulations, like New York's Cybersecurity Regulation, may establish additional requirements with

respect to cybersecurity. In addition, other federal or state laws that do not relate specifically to cybersecurity may include requirements (e.g., privacy requirements) that bear on cybersecurity.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The Computer Fraud and Abuse Act (CFAA) establishes a private cause of action for intentional harm caused by electronic means that covers hacking, denial-of-service attacks, infection of IT systems with malware, and computer-related fraud, among others. Recovery in damages is available for "any impairment to the integrity or availability of data, a program, a system or information" as well as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service". To be actionable, the misconduct must cause at least $5,000 in losses in a one-year period, cause physical injury, affect medical treatment or public health or safety, or affect a computer used by a U.S. government entity in the area of justice, national defence or national security.

The Electronic Communications Privacy Act (ECPA) prohibits unauthorised intentional interception, use, or disclosure of any wire, oral, or electronic communication and permits a person whose wire, oral, or electronic communication is intentionally intercepted, disclosed, or used without authorisation to recover actual and punitive damages, attorneys' fees, litigation costs, and equitable relief.

The Stored Communications Act (SCA) prohibits intentional unauthorised access to stored electronic communications, and unauthorised disclosure of any stored communications by a provider of remote computing services or electronic communication services and relief may include preliminary and other equitable or declaratory relief, actual damages, attorneys' fees, and litigation costs.

As discussed in question 5.3, an Incident may also give rise to claims under a number of state law tort theories.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Many litigated cases relate to Incidents committed by current or former employees of the targeted company who exceed authorisations or violate confidentiality obligations in misappropriating electronic information for use on behalf of a new employer. In such cases, claims have been sustained under the CFAA where the employer could show it was required to take investigative measures that cost more than the $5,000 statutory loss threshold, while other claims have been dismissed for failure to allege sufficient damage. State law claims for misappropriation of trade secrets and unfair competition have also succeeded on such facts.

In *In re Yahoo! Inc. Secs. Litig.*, No. 5:17-cv-00373-LHK (N.D. Cal.), the court approved an $80 million shareholder settlement with Altaba Inc. (formerly Yahoo! Inc.) in response to two class actions against Altaba, alleging that it had violated federal securities laws in its response to data breach Incidents in 2014 and 2016.

In *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), the court issued a preliminary injunction under the CFAA and state law trespass to chattels against a defendant who used a bot to systematically query the plaintiff's domain name registry to compile information for mass marketing. The requisite damage was held to be established by the impairment of the plaintiff's server capacity by the activity of the defendant's bot.

Liability under the ECPA was held to be established and statutory damages of $100 per day of violation awarded, albeit on a default judgment, in *DirecTV, Inc. v. Perrier*, 2004 U.S. Dist. LEXIS 9258 (W.D.N.Y. 2004), where the defendants used an "Unlooper" that was "designed to permit the viewing of plaintiff's television programming without authorisation by or payment to plaintiff" and could not have had any other significant purpose.

In a case involving "a pattern of suspicious logins to numerous subscriber accounts" of a real estate listing website, *Kaufman v. Nest Seekers, LLC*, 2006 U.S. Dist. LEXIS 71104 (S.D.N.Y. Sep. 26, 2006), the court held that the subscribers' ability to email listings to other subscribers or third parties rendered the site an "electronic communication service" protected by the SCA.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Some Incidents may satisfy the elements of the torts of conversion, trespass to chattel, or fraud under state law in New York and likely other states. In *Hecht v. Components International, Inc.*, 867 N.Y.S.2d 889 (Sup. Ct. 2008), involving an ex-employee's unauthorised access to a company's computer system, the court held that deletion of emails or other electronically-stored information could constitute trespass to chattel if it thereby deprived the plaintiffs of the use of such information, or "impaired […] its condition, quality or value", but found that the company failed to establish that the emails deleted by the ex-employee were valuable to the company. With respect to computer systems themselves, the court in *School of Visual Arts v. Kuprewicz*, 771 N.Y.S.2d 804 (Sup. Ct. 2003) held that allegations that the defendant intentionally sent large volumes of unsolicited emails that "depleted hard disk space, drained processing power, and adversely affected other system resources on [plaintiff's] computer system" stated a claim for trespass to chattels.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. Cyber insurance policies are available on a standalone basis, as costs related to Incidents are typically excluded from coverage under general business insurance policies.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory or legal limitations to what cyber insurance policies can cover, though losses due to the insured's failure to remedy known security flaws are typically excluded.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

(a) Employers monitoring their employees are generally subject to the ECPA's prohibition on intentionally intercepting wire, oral or electronic communications while in transit, accessing stored wire or electronic communications, or disclosing or using the contents of such communications.

Two exceptions, however, are commonly applicable to employers:

- the business purpose exception, which permits employers to monitor oral, wire and electronic communications as long as employers can show a legitimate business purpose for doing so; and
- the employee consent exception, which allows employers to monitor employee communications, provided that they have their employees' consent to do so.

(b) There are no specific requirements under Applicable Law regarding the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer. There may be applicable provisions in employer policies or employees' contracts of employment that could create such requirements.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There is no U.S. federal law specific to the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee. However, there are a number of laws protecting whistleblowers in particular contexts that may apply to such reports:

- the Sarbanes-Oxley Act, applicable to reports of fraud and securities violations at publicly traded companies;
- the Dodd-Frank Wall Street Reform and Consumer Protection Act, applicable to reports of securities violations;
- the Occupational Safety and Health Act, applicable to reports of occupational health and safety violations;
- the Financial Institutions Reform Recovery and Enforcement Act, applicable to reports of legal violations at banks and other depository institutions;
- the Energy Reorganization Act, applicable to reports by employees in the nuclear industry of violations of that law, the Atomic Energy Act, or Nuclear Regulatory Commission regulations; and
- the Defend Trade Secrets Act, which applies to employees who disclose a trade secret (a) in confidence to a governmental official or an attorney, solely for the purposes of reporting or investigating a suspected violation of law, or (b) in a document that is filed under seal in a lawsuit or other proceeding.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The U.S. Department of Justice and other sector-specific regulatory authorities have the authority to investigate cybersecurity Incidents. The Department of Justice has broad authority to investigate potential criminal offences. Nevertheless, certain laws, including the Stored Communications Act (SCA), the Wiretap Statute, and the Communication Assistance for Law Enforcement Act (CALEA), provide particular powers or tools that the Department of Justice has at its disposal to investigate possible computer crimes. In response to *United States v. Microsoft*, in which Microsoft objected to the extraterritorial reach of a warrant issued under the SCA, the U.S. government enacted the CLOUD Act in 2018, which expressly provides that a warrant issued under Section 2703 of the SCA can be used to compel a company operating in the U.S. to produce certain electronic communications data within its "possession, custody, or control", regardless of whether that data is stored outside the United States.

Sector-specific regulatory agencies, such as the U.S. Securities and Exchange Commission or the Financial Industry Regulatory Agency, have the authority to investigate, and issue requests for documents and information, relating to Incidents that appear to violate laws, rules or regulations within their purview.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no federal laws that require organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys.

Acknowledgment

In addition to lead authors Keren Livneh and Jacob Reed, Brian Jebb, Partner in Allen & Overy's employment and labour law practice, contributed substantially to the preparation of this chapter. Special thanks as well to associate Kurt Wolfe for his invaluable assistance.

Keren Livneh
Allen & Overy LLP
1221 Avenue of the Americas
New York, NY 10020
USA

Tel: +1 212 610 6300
Email: keren.livneh@allenovery.com
URL: www.allenovery.com

Keren has broad data protection experience spanning transactional and advisory matters. She regularly negotiates privacy-related aspects of acquisitions, as well as data transfer agreements and outsourcing arrangements. Keren counsels on international data transfers and related conflicts of laws, intragroup arrangements, privacy policies, employee monitoring and data breaches. In addition, she has significant experience in intellectual property matters. Keren was included among the Top Women Attorneys in New York Rising Star listing in *The New York Times* (2015 to 2018).

Jacob Reed
Allen & Overy LLP
1101 New York Avenue, N.W.
Washington, D.C. 20005
USA

Tel: +1 202 683 3800
Email: jacob.reed@allenovery.com
URL: www.allenovery.com

Jacob has experience advising international clients on the cyber security and data privacy risks of complex cross-border operations, as well as the legal and operational implications of recent developments in cyber security laws and regulations. Prior to joining Allen & Overy, he spent over a decade at the National Security Agency, where he served for several years as a Technical Director and Mission Manager for NSA's Global Telecommunications Operations office, successfully leading the organisation through an era of rapid technological change and legal reforms. Combining his technical expertise and a thorough understanding of relevant laws and compliance regulations, he helped implement more secure and compliant national security systems and advised federal policymakers on the reform of U.S. cyber security and data privacy laws.

ALLEN & OVERY

Allen & Overy's U.S. cybersecurity and data protection team, led by partners Laura R. Hall and William E. White, is integrated with the firm's global cybersecurity practice to deliver seamless advice on cross-border issues. The U.S. team, like the global cybersecurity practice, spans the numerous practice areas involved in protecting against and responding to potential cybersecurity breaches, including corporate transactions, regulatory compliance, investigations, and litigation. As part of the practice's global scope, the U.S. team regularly advises its international clients on the most recent developments in cybersecurity law and the impact that such developments could have on a client's activities in the U.S. or abroad.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com