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:

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