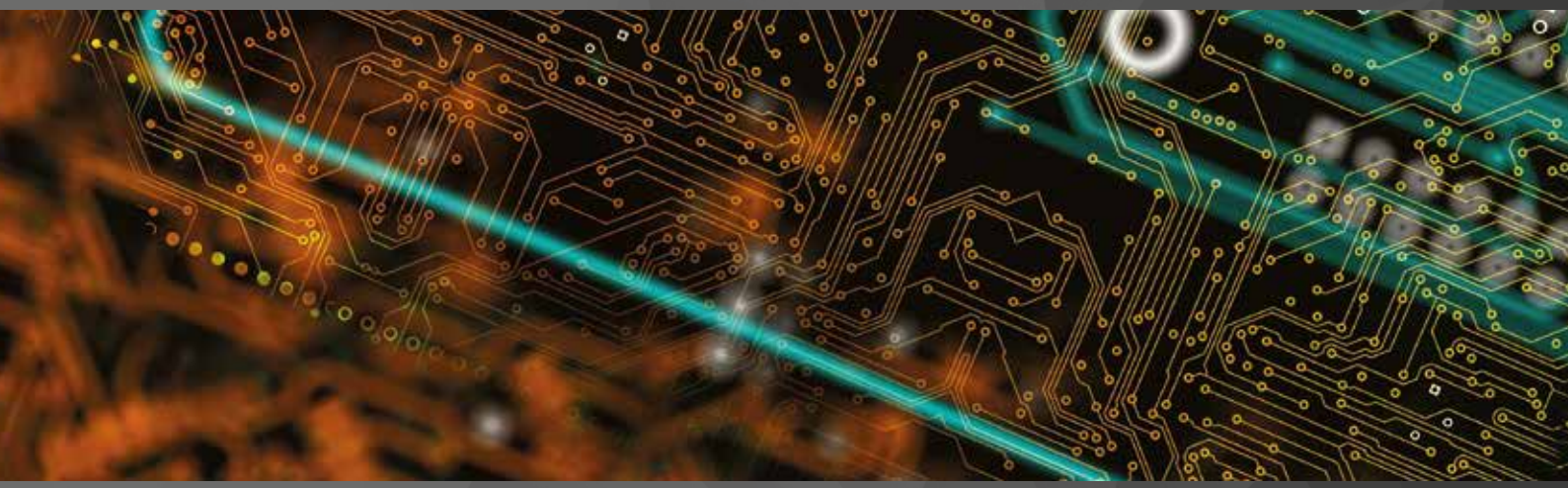
International Comparative Legal Guides



Cybersecurity 2021

A practical cross-border insight into cybersecurity law

Fourth Edition

Featuring contributions from:

Alburhan
Allen & Overy LLP
Ankura Consulting Group
Creel, García-Cuéllar, Aiza y Enríquez
Drew & Napier LLC
Eversheds Sutherland (Germany) LLP
Hamdan AlShamsi Lawyers & Legal Consultants
Ince
Iwata Godo
Kellerhals Carrard
King & Wood Mallesons
Kluge Advokatfirma AS
Lee & Ko
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan LLP
Mori Hamada & Matsumoto
Nikolinakos & Partners Law Firm
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Ropes & Gray LLP
Rothwell Figg
Rubino Avvocati
Schönherr Rechtsanwälte GmbH
Simion & Baciu
Sirius Legal
Stehlin & Associés
TIME DANOWSKY Advokatbyrå AB

ICLG.com

Expert Chapters

1 **Get Stuffed! Are You Prepared for a Credential-Stuffing Attack?**
Nigel Parker & Nathan Charnock, Allen & Overy LLP

5 **Current and Emerging Cybersecurity Threats and Risks**
Robert Olsen, Daron M. Hartvigsen & Brandon Catalan, Ankura Consulting Group

10 **Phantom Responsibility: How Data Security and Privacy Lapses Lead to Personal Liability for Officers and Directors**
Christopher Ott, Rothwell Figg

20 **Mitigating Cyber-Risk – A Boardroom Priority**
Rory Macfarlane, Ince

24 **Why AI is the Future of Cybersecurity**
Akira Matsuda & Hiroki Fujita, Iwata Godo

Q&A Chapters

28 **Australia**
Nyman Gibson Miralis: Dennis Miralis, Phillip Gibson & Jasmina Ceic

35 **Austria**
Schönherr Rechtsanwälte GmbH: Christoph Haid, Veronika Wolfbauer & Michael Lindtner

42 **Belgium**
Sirius Legal: Roeland Lembrechts & Bart Van den Brande

49 **Canada**
McMillan LLP: Lyndsay A. Wasser & Kristen Pennington

58 **China**
King & Wood Mallesons: Susan Ning & Han Wu

67 **England & Wales**
Allen & Overy LLP: Nigel Parker & Nathan Charnock

75 **France**
Stehlin & Associés: Frédéric Lecomte

82 **Germany**
Eversheds Sutherland (Germany) LLP: Dr. Alexander Niethammer, Constantin Herfurth, Dr. David Rieks & Stefan Saerbeck

89 **Greece**
Nikolinakos & Partners Law Firm: Dr. Nikos Th. Nikolinakos & Dina Th. Kouvelou

98 **Ireland**
Maples Group: Claire Morrissey & Kevin Harnett

105 **Israel**
Pearl Cohen Zedek Latzer Baratz: Haim Ravia & Dotan Hammer

112 **Italy**
Rubino Avvocati: Alessandro Rubino & Gaetano Citro

120 **Japan**
Mori Hamada & Matsumoto: Hiromi Hayashi, Masaki Yukawa & Daisuke Tsuta

129 **Korea**
Lee & Ko: Hwan Kyoung Ko & Kyung Min Son

136 **Mexico**
Creel, García-Cuéllar, Aiza y Enríquez: Begoña Cancino

142 **Norway**
Kluge Advokatfirma AS: Stian Hultin Oddbjørnsen, Ove André Vanebo, Iver Jordheim Brække & Mari Klungsøyr Kristiansen

149 **Poland**
Leśniewski Borkiewicz & Partners (LB&P): Mateusz Borkiewicz, Grzegorz Leśniewski & Jacek Cieśliński

158 **Romania**
Simion & Baciu: Ana-Maria Baciu, Cosmina Maria Simion, Andrei Cosma & Andrei Nicolae Dumbravă

166 **Saudi Arabia**
Alburhan: Saeed Algarni, Mohammed Ashbah & Muhanned Alqaidy

172 **Singapore**
Drew & Napier LLC: Lim Chong Kin, David N. Alfred & Albert Pichlmaier

182 **Sweden**
TIME DANOWSKY Advokatbyrå AB: Jonas Forzelius & Esa Kymäläinen

189 **Switzerland**
Kellerhals Carrard: Dr. Oliver M. Brupbacher, Dr. Nicolas Mosimann & Marlen Schultze

199 **Taiwan**
Lee and Li, Attorneys-at-Law: Ken-Ying Tseng

206 **Thailand**
R&T Asia (Thailand) Limited: Supawat Srirungruang & Saroj Jongsaritwang

214 **United Arab Emirates**
Hamdan AlShamsi Lawyers & Legal Consultants: Hamdan Al Shamsi & Helen Tung

220 **USA**
Ropes & Gray LLP: Edward R. McNicholas & Kevin J. Angle

England & Wales


Nigel Parker


Nathan Charnock

Allen & Overy LLP

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative 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. If a person commits this offence with the intent to commit or facilitate a more serious "further offence" (e.g. theft via the diversion of funds), the maximum penalty is five years' imprisonment. In 2019, a director of a CCTV provider and her employee were sentenced to 14 months' and five months' imprisonment (respectively) after they accessed CCTV footage of the post-mortem of footballer Emiliano Sala. In 2019, a disgruntled former IT contractor at Jet2 was sentenced to 10 months' imprisonment after he deleted user accounts and accessed the email account of the Jet2 CEO in a revenge attack.

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. In 2017 and 2019, two individuals were each sentenced to 16 months in youth offender institutions for separate denial-of-service attacks against various websites targeting websites of law enforcement and a number of companies including Amazon, Netflix and NatWest.

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.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
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.

Under the Fraud Act 2006, it is an offence to make or supply articles for use in the course of, or in connection with fraud, provided the individual either has (i) knowledge that the article is designed or adapted for use in the course of or in connection with fraud, or (ii) intends the article to be used to commit or assist in the commission of fraud. On indictment, the maximum penalty is 10 years' imprisonment.

In 2019, an individual was sentenced to nine years' imprisonment after he created website scripts designed to look like the websites of up to 53 UK-based companies to help criminals defraud victims out of approximately £41.6 million. He also supplied the criminals with software that disguised their phishing sites from being identified by web browsers.

Possession or use of hardware, software or other tools used to commit cybercrime
Yes. See the response relating to the distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime above.

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 2019, an individual was convicted of offences under the Fraud Act 2006 and Computer Misuse Act 1990 (after accessing a barrister colleague's email account to copy his practising certificate in order to produce a faked copy in his own name before going on to practice as a barrister working on 18 cases) and was sentenced to a total of two years' and three months' 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. In 2020, a self-employed IT support specialist was sentenced to 20 months' imprisonment for offences under the Computer Misuse Act 1990 and the Theft Act 1990 after he stole over £31,000 in cryptocurrency from a client.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Yes. See "Hacking (i.e. unauthorised access)" 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
Please see above. In addition, 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.

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 factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

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. However, Crown Prosecutors will consider a number of public interest factors before charging an individual with an offence.

2 Cybersecurity Laws

2.1 *Applicable Law*: 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, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

England and Wales does not have a comprehensive cybersecurity law; instead, the legal framework for cybersecurity is dispersed across a number of different laws:

- **Data Protection Act 2018** – applies, alongside the EU General Data Protection Regulation insofar as it forms part of retained EU law in the UK following Brexit (**UK GDPR**), to Incidents to the extent that they involve Personal Data. The Data Protection Act 2018 also sets out data protection requirements for national security and immigration as well as other domestic areas of law.
- **Communications Act 2003** – includes cybersecurity obligations that apply in the telecommunications sector to public electronic communications network providers and public electronic communications service providers.
- **Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)** – includes security obligations in respect of personal data that apply to public electronic communications service providers.
- **The Network and Information Systems Regulations 2018 (NIS Regulations)** – implements the EU Network and Information Systems Directive into UK law, imposing obligations on operators of essential services (**OES**) and relevant digital service providers (**RDSPs**). OES are organisations that operate services deemed critical to the economy and wider society such as water, transport, energy, healthcare and digital infrastructure. RDSPs are anyone who provides online marketplaces, online search engines or cloud computing services and, is a medium or large-sized business with its head office, or a nominated representative in the UK. The NIS Regulations require OES and RDSPs to have sufficient security systems in place to prevent the data they hold or the services they provide being compromised and to report certain Incidents to a competent authority. The ICO is the competent authority for RDSPs. See question 2.2 for more information about OES.
- **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 answers to question 1.1), which may be prosecuted in conjunction with offences under the **Theft Act 1968** or the **Fraud Act 2006**.
- **Official Secrets Act 1989** – may 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.
- Governance obligations, which can directly or indirectly relate to cybersecurity, apply to public companies under the **Companies Act 2006**, the Disclosure and Transparency Rules and the Listing Rules in the **Financial Conduct Authority (FCA) Handbook** and the risk management and control provisions in the **UK Corporate Governance Code**.
- Various common law doctrines may also apply in respect of civil actions (see question 5.1).

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

- **Telecommunications sector** – cybersecurity requirements under the Communications Act 2003 require providers of

public electronic communications networks and public electronic communications services to, amongst other things, maintain the security and integrity of those networks and services, including by taking measures to prevent or minimise the impact of Incidents on end users and on the interconnection of networks.

- **Operators of essential services (OES)** – The NIS Regulations came into force in the UK on 10 May 2018, imposing certain security duties, on any "operator of essential services", 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 NIS Regulations also place obligations on digital service providers in relation to security and reporting of Incidents. The NCSC does not have a regulatory function but it will undertake the role of the Computer Security Incident Response Team responding to Incidents which arise as a result of a cyber-attack and which have been notified to it. The NIS Regulations introduce a range of penalties that can be imposed by the relevant competent authority. These range from £1 million for any contravention of the NIS Regulations which the relevant authority determines could not cause an Incident, up to £17 million for a material contravention of the NIS Regulations which 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.
- **Financial services sector** – The Senior Management Arrangements Systems and Controls (**SYSC**) part of the FCA Handbook (see answer to question 3.2) applies to financial services infrastructure providers who are regulated by the FCA – these organisations will be operators of essential services for the purposes of the NIS Regulations (see above).

2.3 *Security measures*: Are organisations required under Applicable Laws 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 UK GDPR), if an organisation is a 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 and 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 personal data. Controllers are also required to document any personal data breaches.

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 its 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 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) 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; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Data Protection Act 2018 and UK GDPR

Under the Data Protection Act 2018 and the UK GDPR, a 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; (b) the name and contact details of the organisation's data protection officer or contact point; (c) the likely consequences of the Incident; and (d) the measures taken, or proposed to be taken, to address the Incident and mitigate possible adverse effects.

Under the Data Protection Act 2018, the ICO is not permitted to publicise any information that has been disclosed to it (e.g. 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).

NIS Regulations

The NIS Regulations also require OES and RDSPs 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.

The NCSC publishes a weekly threat report on its website, with content drawn from recent open source reporting, which details cyber threat information, known network and software vulnerabilities and other information organisations and individuals may find useful. However, there is no obligation for organisations to report threat information to the NCSC to compile these reports.

Communications Act 2003

The Communications Act 2003 requires public electronic communications network providers to notify Ofcom of any breach of security that has a significant impact on the network's operation. It also requires public electronic communications service providers to notify Ofcom of any breach of security that has a significant impact on the operation of the service.

PECR

PECR requires a public electronic communications service provider to 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) and the date and time of detection; (c) information about the nature of the breach; and (d) the nature and content of the personal data concerned and the security measures applied to it.

FCA and PRA Handbooks

An organisation regulated by the FCA are also required to notify the FCA of any significant failure in its 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, the FCA expects payment service providers to comply with European Banking Authority guidelines on major Incident reporting under which those providers are expected 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 to have returned to normal.

2.5 *Reporting to affected individuals or third parties*: 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 UK GDPR, a 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) contact details where more information can be found; (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 its 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 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 personal data that has been breached was encrypted or was rendered unintelligible by similar security measures.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

- The **ICO** is the relevant regulator under data protection laws, including the Data Protection Act 2018, the UK GDPR and PECR (https://ico.org.uk/).
- **Ofcom** is the relevant regulator under the Communications Act 2003 (https://www.ofcom.org.uk/).
- The **FCA** is the relevant regulator under the FCA Handbook (https://www.fca.org.uk/). The **PRA** is also responsible for the regulation and supervision of financial services firms.
- **Sector-based competent authorities** are the relevant regulators in Schedule 1 to the NIS Regulations (https://www.legislation.gov.uk/uksi/2018/506/schedule/1/made).

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

- Data Protection Act 2018 and the UK 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 €10 million.
- 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.

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

In July 2019, in the first fine to be announced by the ICO under the UK GDPR, the ICO announced an intention to issue a fine of £183.39 million to British Airways following an Incident in September 2018. This Incident in part involved user traffic to the British Airways website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers. Personal data of approximately 500,000 customers was compromised in this Incident, which is believed to have begun in June 2018.

Also in July 2019, the day after the announcement of the British Airways fine, the ICO announced further plans to fine Marriott International £99.2 million following a data breach affecting Marriott subsidiary Starwood's guest reservation database. A variety of personal data contained in approximately 339 million guest records globally were exposed by the Incident, of which 7 million related to UK residents. It is believed the relevant vulnerability began in 2014, but was not discovered until 2018. The ICO found that Marriott failed to undertake sufficient due diligence when it bought the Starwood hotels group in 2016, and should have done more to secure its systems.

Both British Airways and Marriott had the opportunity to make further representations to the ICO. It is expected that the fines issued will ultimately be lower than those stated in 2019, but at the time of writing, no further update has been announced by the ICO.

In January 2020, the ICO issued a fine of £500,000 to DSG Retail Limited after security failings enabled malware to be installed by an attacker on 5,390 tills at DSG's Currys, PC World and Dixons Travel stores between July 2017 and April 2018 resulting in unauthorised access to the personal information of approximately 14 million people – this incident occurred prior to the introduction of the UK GDPR and the fine represents the maximum penalty available under the Data Protection Act 1998.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There are no specific laws prohibiting the use of web beacons in the UK. However, where use of a web beacon involves processing personal data, the organisation's use of the web beacon must be in accordance with the requirements of data protection laws.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There are no specific laws prohibiting the use of honeypots in the UK.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There are no specific laws prohibiting the use of sinkholes in the UK.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Monitoring of employees, e.g. monitoring use of email and internet access, involves processing of personal data and so the Data Protection Act 2018 (and the UK GDPR) will apply. The ICO's Employment Practices Code (the **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. A failure to comply with the Code will not automatically result in a breach of the UK GDPR or 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.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

There are no specific restrictions on the import or export of technology designed to prevent or mitigate the impact of cyber-attacks.

However, export authorisation is required for the export of certain technology or software (e.g. decryption technology) that is used for or in connection with, or required for the development, production, or use of, certain explosives, aircraft, firearms, chemicals and vessels.

4 Specific Sectors

4.1 Does market practice with respect to information security 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.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

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 Tesco Bank (£16.4 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 the telecommunications sector, public electronic communications network providers and public electronic communications service providers must take appropriate technical and organisational 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.

5 Corporate Governance

5.1 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' or officers' duties in your jurisdiction?

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. 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.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (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 audit. 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 UK Corporate Governance Code, as applicable from 1 January 2019, emphasises the board's responsibility to determine and assess the principal risks facing the company. This responsibility extends to a robust assessment of the company's emerging risks, which would cover cyber risk.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) 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 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.

6 Litigation

6.1 Please provide details of any civil or other private 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.** Where there is unauthorised disclosure or use of information and: (i) the information itself had a necessary quality of confidence about it; (ii) that information was imparted in circumstances importing an obligation of confidence; and (iii) there was an unauthorised use of that information to the detriment of the party communicating it.
- **Breach of contract.** This could take any form, including a breach of a commercial contract or breach of an employee's terms and conditions of employment. For example, 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 they have 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. 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.
- **Causing loss by unlawful means.** A defendant will be liable for causing loss by unlawful means where they intentionally cause 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 UK 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 UK GDPR) are entitled to compensation for that damage. "Non-material damage" includes distress. 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 or 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 suffers loss as a consequence.
- **Directors' duties.** See answer to question 4.1.
- **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 1988, 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 unlawfully to manipulate data on a computer may amount to trespass to that computer.

6.2 Please cite any specific examples of published civil or other private actions 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 had been 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 2018 (and UK GDPR)

Wm Morrisons Supermarket PLC v Various Claimants [2020] UKSC 12: although determined under the previous legislation, in the first group litigation data breach case to come before the courts, Morrisons Supermarket was, following an appeal, found not 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. At first instance, 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. However, this position was overturned on appeal to the Supreme Court.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Please see the list in response to question 6.1.

7 Insurance

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

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

7.2 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.

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 laws. 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 (amongst 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 fully in force (at the time of writing), 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 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.
Nigel is recognised in *Chambers* and *The Legal 500*. He was named one of the "Top 40 under 40" data lawyers by *Global Data Review*.

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

Nathan Charnock is an associate specialising in commercial contracts, data protection and privacy, intellectual property and information technology law. He advises clients on their response to cybersecurity attacks, including their interactions with regulators and implementation of remediation steps. Nathan also advises on complex commercial arrangements for a range of clients in the technology, retail, telecommunication, life sciences and financial services sector, including IP licensing, outsourcing and service provision arrangements.

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

Tel: +44 203 088 3899
Email: nathan.charnock@allenovery.com
URL: www.allenovery.com

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 over 40 offices. 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 19 partners with diverse backgrounds in data protection, bank regulation, anti-trust, 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.

www.allenovery.com

ALLEN & OVERY

ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
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
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by: global legal group