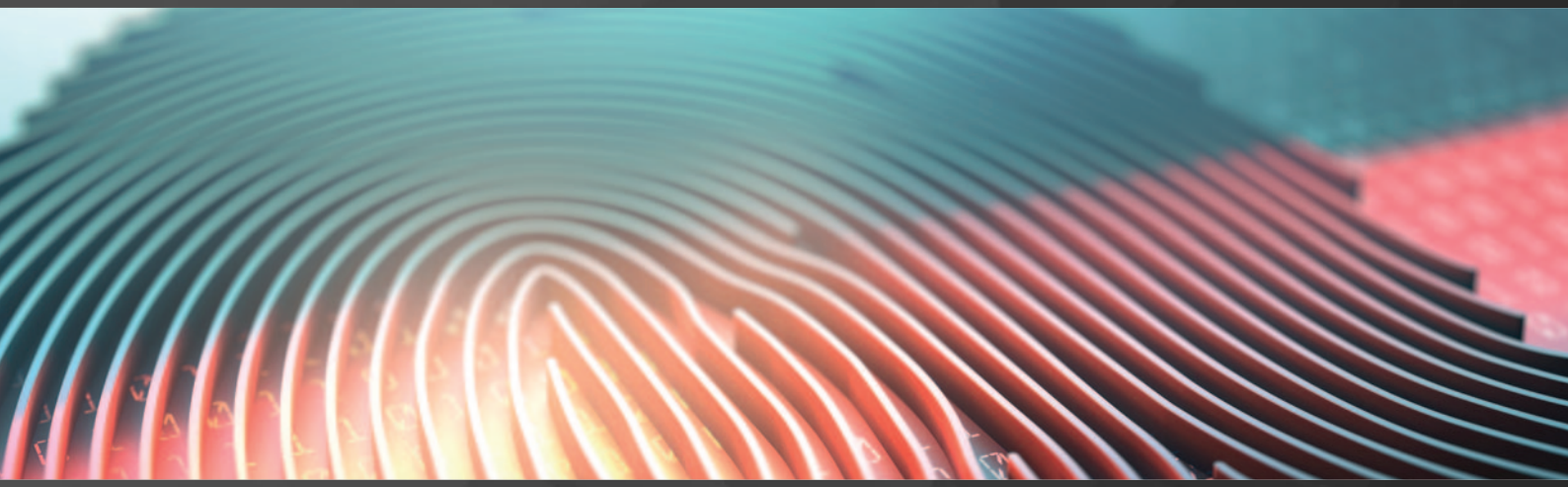
International Comparative Legal Guides



Cybersecurity 2020

A practical cross-border insight into cybersecurity law

Third Edition

Featuring contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Boga & Associates
Christopher & Lee Ong
Cliffe Dekker Hofmeyr
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Faegre Baker Daniels
G+P Law Firm
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P., R.L.
Iwata Godo
King & Wood Mallesons
Lee & Ko
Lee and Li, Attorneys-at-Law
LEĜA
Lesniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Ropes & Gray
SAMANIEGO LAW
Shardul Amarchand Mangaldas & Co.
Siqueira Castro – Advogados
Sirius Legal
Stehlin & Associés
Synch

ICLG.com

England & Wales

Nigel Parker

Alexandra Rendell

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:

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

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

Phishing
Yes. See the answer in respect of hacking.

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

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes. See the answer in respect of denial-of-service attacks.

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

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

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

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

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

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

Yes. For certain offences under the Computer Misuse Act 1990 (such as hacking, phishing or denial-of-service attacks), the offence will be committed where there is a "significant link to the domestic jurisdiction". This includes the person committing the offence being in the UK, the target computer being in the UK or a UK national committing the offence while outside the UK (provided in the latter instance that the act was still an offence in the country where it took place).

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

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

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

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

2 Applicable Laws

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

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

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

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

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

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

The NIS Regulations were published in the UK on 19 April 2018 and came into force on 10 May 2018. The NIS Regulations provide than an 'operator of essential services' must comply with certain security duties, including a duty to notify Incidents to the relevant competent authority. The NIS Regulations identify sector-based competent authorities (for sectors covering energy, transport, health, drinking water supply and distribution and digital infrastructure) with the National Cyber Security Centre (**NCSC**) as the UK's single point of contact for Incident reporting. The NCSC will also undertake the role of the Computer Security Incident Response Team.

However, the NCSC will not have a regulatory function and, in its role as the Computer Security Incident Response Team, will only respond to Incidents which arise as a result of a cyber-attack and which have been notified to it by the competent authorities. The NIS Regulations introduce a range of penalties that can be imposed by the relevant competent authority or the ICO (in the case of digital service providers). These range from £1 million for any contravention of the NIS Regulations 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. This maximum fine is broadly aligned to the maximum level of fine under the GDPR.

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

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

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

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

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

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

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

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (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.

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

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

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

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.

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

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

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

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

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

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

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

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

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

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

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

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

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

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

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

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

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

Under the Data Protection Act 2018 and the GDPR, failure to report an Incident involving a personal data breach, or to implement appropriate security measures, can incur a fine of up to the higher of 2% of annual worldwide turnover or EUR10 million.

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

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

In October 2016, the ICO issued a then-record £400,000 fine to telecoms company TalkTalk for security failings that allowed a cyber

attacker to access customer data. The ICO investigation found that the attack took advantage of a technical weakness in TalkTalk's systems which could have been prevented if TalkTalk had taken 'basic steps' to protect customer data.

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

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

In July 2019, in the first fine to be announced by the ICO under the 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 were 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 seven 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.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks 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 Specific Sectors

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

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

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

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

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

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

4 Corporate Governance

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

Directors are required, under the Companies Act 2006, to promote the success of the company for the benefit of its members as a whole and exercise reasonable skill, care and diligence in performing their role. It is up to the board of directors of each company to ensure that the board has the relevant competence and integrity to exercise these duties in view of the risk to the company as a whole,

including the risk of Incidents. A failure to prevent, mitigate, manage or respond to an Incident may be a breach of directors' duties if, for example, the failure resulted from a lack of skill, care and diligence on the part of the relevant director.

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

No, there are no specific requirements in this respect. However, listed companies are required, under the UK Corporate Governance Code, to set up certain committees with responsibility for specific areas, such as 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, which was updated 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.

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

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

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

No, there are no other specific requirements.

5 Litigation

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

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

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

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

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

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

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

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

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

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

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

Directors' duties. See the answer to question 4.1.

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

Infringement of copyright and/or database rights. Copyright is infringed when a person, without authority, carries out an infringing act under the Copyright, Designs and Patents Act 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.

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

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

Breach of confidence and various economic torts

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

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

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

Please see the list in response to question 5.1.

6 Insurance

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

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

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

No, there are no regulatory limitations.

7 Employees

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

Monitoring of employees, for example, monitoring use of email and internet access, involves processing of personal data and so the Data Protection Act 2018 (and the GDPR) will apply. The ICO's Employment Practices Code (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. This notification should include details of the circumstances in which monitoring will take place, the nature of the monitoring, how the information will be used and what safeguards are in place for the employees. A failure to comply with the Code will not automatically result in a breach of the Data Protection Act 2018. However, an organisation should be able to justify any departure from the Code, and the ICO can take this into account in consideration of any enforcement action.

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

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

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

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

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

8 Investigatory and Police Powers

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

Law enforcement authorities have various surveillance powers under UK 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 (among others), provided this is proportionate and the information could not reasonably be obtained by other means. Under the Investigatory Powers Act 2016, new warrants are available for targeted equipment interference and targeted examination, as well as bulk warrants to enable law enforcement to obtain the communications data of multiple individuals using one warrant.

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

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

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

Nigel Parker 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

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

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

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

Allen & Overy is a full-service global elite law firm headquartered in London. Our commitment to help our clients deliver their global strategies has seen us build a truly global network now spanning 44 offices in 31 countries. We have also developed strong ties with relationship law firms in more than 100 countries where we do not have a presence.
We have a strong cybersecurity practice comprising a core team of 15 partners with diverse backgrounds in data protection, bank regulation, 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