CYBERSECURITY 2022

In association with
Simmons & Simmons

LEXOLOGY
Getting the Deal Through

simmons+simmons

simmons+simmons

Our team provides a business-focused and pragmatic approach.

Our international data, privacy and cybersecurity practice spans the globe advising within the Asset Management & Investment Funds, Financial Institutions, TMT and Healthcare & Life Sciences sectors.

Our lawyers advise on the full suite of data and cybersecurity issues – from implementing preventative measures and regulatory requirements through to data breach response and full-scale litigation.

simmons-simmons.com

United Kingdom

Robert Allen, Lawrence Brown, Neil Westwood, Russell Cowie and Emily May*

Simmons & Simmons

LEGAL FRAMEWORK

Legislation

1 | Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The UK does not have a comprehensive cybersecurity law – instead, cybersecurity requirements and obligations are set out in various legislation:

- The Network and Information Systems Regulations 2018 (NISR) impose security and incident reporting requirements on organisations that are operators of essential services (OESs) and relevant digital service providers (RDSPs). An RDSP is an online marketplace, online search engine, or cloud computing service provider established in, or with a representative established in, the UK and which is not a micro or small enterprise. These organisations must have proportionate and effective security measures and procedures to ensure continuity of business services and effective incident reporting. The UK government is consulting on expanding the range of digital service providers affected by the NISR to include other types of digital services.
- The Communications Act 2003 (CA 2003) requires public electronic communications services (ECS) and electronic communications network (ECN) providers to ensure the security of their networks and services, including incident mitigation.
- The Telecommunications (Security) Act 2021 (TSA) amends the CA 2003 and will impose new legally binding security requirements on ECN and ECS providers. The provisions of the TSA that provide new powers to legislators and regulators are currently in force, with the provisions relating to the obligations on providers due to be introduced by way of statutory instrument.
- The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) impose data security requirements on controllers and processors of personal data, and prescribe a risk-based approach to data security.
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) place further obligations on ECS providers.

In respect of the financial services sector, the FCA Handbook also imposes a number of cybersecurity requirements on firms through its governance obligations.

2 | Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Publicly listed companies and those within the financial services sector are subject to governance and security requirements which, either directly or indirectly, impose cybersecurity obligations upon them. The enforcement action that may be taken against such organisations can include significant fines and other sanctions, and there is significant reputational risk associated with such measures.

Operators of essential services (including in the energy, transport and health sectors) and digital service providers are subject to the additional cybersecurity and reporting obligations under the NISR. These organisations must implement appropriate technical and organisational measures to manage the cybersecurity risks to their networks and systems, and adopt measures that will enable them to mitigate the impact of incidents.

The UK government's National Cyber Strategy 2022 (the Strategy) highlights the interaction between established sectors of the economy and new and unregulated businesses (such as electric vehicle charging or those that provide microgeneration) as an area of potential concern, with the diversification of the business landscape likely to result in fundamental changes to the regulatory approach to cybersecurity.

There are not currently any cybersecurity obligations that apply explicitly to professionals in the legal sector; however, firms will be subject to broader data protection legislation such as the GDPR when conducting their business.

3 | Has your jurisdiction adopted any international standards related to cybersecurity?

There are no mandatory ISO standards in the United Kingdom. However, organisations may adopt standards such as ISO 27001:2013 to evaluate which security measures are required to meet their obligations under the NISR. Similarly, adherence to the standards is a means by which data controllers can demonstrate compliance with their obligations under the GDPR and DPA 2018.

Organisations also frequently elect to adopt ISO standards through contractual provisions, to demonstrate that their cybersecurity policies and procedures are sufficiently robust.

4 | What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

There is no legislation that imposes direct responsibility for cybersecurity compliance on personnel and directors. However, directors of organisations that fail to adequately ensure cybersecurity may be held responsible under the Companies Act 2006, which requires directors to exercise reasonable skill, care and diligence in the performance of their functions.

5 | How does your jurisdiction define cybersecurity and cybercrime?

The UK government's Strategy defines cybercrime as crime that can only be committed through the use of ICT devices, or which are changed

significantly (in scale and reach) by the use of ICT. The Strategy defines cybersecurity as the protection of internet-connected systems (including hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse.

The NISR relate to the security of network and information systems and therefore amount to cybersecurity obligations. However, information security requirements under the NISR also include other system and environmental considerations (such as management of system failure, human error, and natural events).

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The UK GDPR does not prescribe specific security measures that organisations must have in place; firms must implement appropriate technical and organisational measures to ensure the security of personal data, which may include measures such as encryption or pseudonymisation of data.

Organisations that fall within the NISR must also take appropriate and proportionate technical and organisational measures to ensure that risks to their systems are managed. In addition, the NISR provide for obligations relating to:

- the security of network and information systems and facilities;
- incident handling (including detection procedures and incident reporting);
- business continuity management (including disaster recovery capabilities);
- monitoring, auditing and testing (including processes to reveal flaws in the security mechanisms used to protect the network and information systems); and
- compliance with international standards relating to the security of network and information systems.

Scope and jurisdiction

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

There is no legislation that specifically addresses cyberthreats to intellectual property. However, the Strategy specifically identifies the protection of intellectual property in critical cyber technologies as an objective, with a particular focus on the sectors mentioned in the National Security and Investment Act 2021 (NSIA), including artificial intelligence, communications, and cryptographic authentication.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The NISR apply to operators of essential services in a number of sectors (including energy, transport and health) and provides that organisations must take appropriate and proportionate technical and organisational measures to manage risks posed to their network and information systems, including measures to mitigate the impact of incidents. The NISR also impose reporting standards on these organisations, with mandatory notification to the relevant authority within 72 hours of becoming aware of an incident occurring. Compliance with the NISR is actively monitored by the designated authorities (including the Information Commissioner's Office (ICO)) and the UK has adopted an audit framework in respect of OESs and RDSPs to ensure compliance with the relevant requirements.

In respect of the financial services sector, the Senior Management Arrangement Systems and Controls (SYSC) section of the FCA Handbook applies to providers of financial services infrastructure, and requires firms to have effective and proportionate risk-based systems to combat financial crime.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

The Investigatory Powers Act 2016 (IPA) criminalises the unlawful interception of communications within the UK. The IPA also limits the sharing of information lawfully obtained by UK law enforcement bodies and intelligence agencies via interception. It is a criminal offence under the IPA for communication service providers or public officials to disclose the existence and content of a warrant or authorisation where a government agency has, under a bulk or targeted warrant, intercepted communications in the interests of national security or for the prevention of serious crime.

The Counter-Terrorism Act 2008 covers disclosure of information to the intelligence services for the purposes of national security or the prevention of serious crime.

The UK GDPR and the DPA 2018 only permit personal data sharing to law enforcement authorities where it is necessary and proportionate. Except where the ICO determines that publication is in the public interest, the ICO is prohibited from publicising information disclosed to it via a personal data breach notification that relates to any identifiable individual or business that is not already in the public domain.

Article 8 of the Human Rights Act, which deals with an individual's right to privacy, can be interfered with by a public authority only where it can be shown that such interference is lawful, necessary, and proportionate to protect national security.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The Computer Misuse Act 1990 (CMA) is the primary cybercrime legislation in the UK. The CMA criminalises unauthorised access to computer networks, such as hacking; intention to commit a cybercrime; modifying, removing, or ransoming data; and aiding computer misuses.

Section 3 of the IPA criminalises the unlawful interception of communications within the UK.

In relation to personal data processing, the DPA 2018 creates a number of offences, such as unlawfully obtaining personal data, knowingly or recklessly disclosing personal data without the consent of the data controller, and the sale of personal data obtained illegally. Fraud by false representation, which could cover certain phishing incidents, is punishable under the Fraud Act 2006.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

The NISR specifically govern certain categories of digital services, including cloud computing services, and aim to establish a common level of security for network and information services.

The NSIA allows the government to scrutinise and intervene in acquisitions of control of companies involved in 17 'sensitive areas of the economy', where there is a potential impact on the UK's national security. One such area is cloud computing. The rules came into force on 4 January 2022, although they can be enforced retrospectively for deals that were completed on or after 12 November 2020. Completion of a notifiable acquisition without approval could lead to criminal or civil penalties.

The UK's National Cyber Security Centre (NCSC) offers a framework to organisations in the UK public sector built around 14 Cloud Security Principles that cover how organisations should configure, deploy, and use cloud services securely.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The NISR apply to OESs and RDSPs outside of the UK that offer services in the UK, and require these organisations to nominate a representative to the relevant competent authority for enforcement purposes.

The CMA has extraterritorial effect in relation to offences with a significant link to the UK (ie, where the accused was in the UK when the offence was committed, the unauthorised action was committed, or the target computer was located in the UK). The Serious Crime Act 2015 amended the CMA to provide for additional extraterritorial powers where there is a significant link. A significant link is established if the conduct in question caused serious damage of a material nature in the UK. Additionally, if the accused is a UK national and commits an offence while outside of the UK under the law of another country then a significant link is established.

The IPA also provides for extraterritorial application in respect of communications carried out in the UK (ie, where an individual in the UK is communicating with persons in other jurisdictions). UK law enforcement agencies may issue warrants under the IPA to overseas service providers for data, the interception of communications or the monitoring of computer equipment.

Foreign organisations will be subject to the UK GDPR, including its security requirements, if they offer goods or services to individuals in the UK. Personal data transferred from UK to organisations in third countries must be subject to appropriate safeguards, which typically involves the execution of standard data protection clauses, including provisions covering security measures, between the exporting and importing organisation. In February 2022, the ICO published a new form of International Data Transfer Agreement to be used for this purpose (subject to parliamentary approval). At the time of writing, further ICO guidance on use of the IDTA and the conduct of data transfer risk assessments is anticipated.

BEST PRACTICE

Increased protection

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

Enhanced cybersecurity protections, beyond those mandated by law, are recommended by a number of different authorities, with guidance notes and advice widely available.

The National Cyber Security Centre (NCSC) is an organisation within the UK government that provides advice and support for the public and private sector to promote cybersecurity. The central pillar of its advice is '*Cyber Aware*', which provides a set of guidelines built around six key actions. In addition, it also maintains '*10 Steps to Cyber Security*', guidance aimed at medium-sized to large organisations that employ cybersecurity professionals, and a *'Small Business Guide: Cyber Security*'. On top of this, the NCSC publishes various focused guides on passwords, ransomware, phishing, devices, personal data malware, operational security and the cloud.

Other authorities also recommend enhanced protections. The Global Cyber Alliance, Action Fraud, the Information Commissioner's Office (ICO) and the Financial Conduct Authority (FCA) are among other authorities that also recommend protections beyond those strictly mandated by law.

It should be noted that while industry and regulatory codes or guidance do not constitute protections mandated by law, failure to follow such codes may still give rise to adverse consequences. For example, the ICO states, in its Regulatory Action Policy, that failure to follow an approved or statutory code of conduct is an aggravating factor when it considers sanctions.

14 How does the government incentivise organisations to improve their cybersecurity?

Following a 2019 consultation, on 19 January 2022 the government published a policy paper entitled '2022 cyber security incentives and regulation review'. In that it noted that it was for the market to incentivise better security practices for organisations, but recognised that those incentives (such as consumer pressure and competitive advantage) have not yet formed effectively. To mitigate this, the government plans to take a more interventionalist approach through guidance, further market participations and strengthening of UK cyber legislation.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The NCSC publishes a guide dealing with issues such as cyber defence, threat and ransomware. The NCSC's *10 Steps to Cyber Security* sets out a number of key areas for medium-sized to large organisations to ensure that technology, systems and information are protected against cyberattacks. In doing so the guide emphasises the need to take a risk-based and proactive approach to cybersecurity.

Organisations operating within the regulated financial services sector are also guided by a range of materials produced by the FCA in order to achieve compliance with its Principles, and the standards set out in the SYSC sourcebook. One such example is the FCA's publication on *Good cyber security – the foundations*, which demonstrates the FCA's approach to working with other organisations (namely, the NCSC) in order to achieve effective levels of cybersecurity within the sector.

16 Are there generally recommended best practices and procedures for responding to breaches?

The best way to mitigate the impact of a data breach is to ensure you are properly prepared. A number of public organisations have published guidance for responding to data breaches (including the ICO and the NCSC). You should already have a detailed cybersecurity policy and within that should be a data breach response plan. Such a plan should be accessible to all employees and form part of standard onboarding training.

The first recommended step is to identify the extent of the breach and preserve relevant evidence. Although basic, it is important to document how the breach was identified and keep a careful note of steps taken. Such steps might include ensuring the correct internal stakeholders have been contacted (eg, HR, security), determining whether the breach contained personal data, and identifying

which jurisdictions may have been affected. Answering these questions will inform the scope of external bodies that need to be involved in the crisis response team (eg, forensic experts to track the extent of the breach).

Next, your focus should shift to analysis, that is, understanding the 'how'. For example, how did the breach occur and is it ongoing? If so, what steps need to be taken to fix (or 'patch') the breach? At this stage, you should consider whether stopping the breach might 'tip off' the attacker and lead to the destruction of evidence; this should be balanced against your data protection duties. You should also consider any external and internal communications. For example, you might want to consider a formal press release, or an internal notice reminding employees of the sensitivities of publicly discussing the breach with the media.

You should then consider the remedies and next steps available to you. Depending on the circumstance of the breach, this can range from initiating legal action to instigating a PR strategy.

Finally, you should consider your long-term response. If the breach identified any holes in your security system or staff training, these should be addressed as a matter of urgency. You should also reflect on whether you need to strengthen the relationships with necessary third parties; you may want, for example, to have forensic experts or legal counsel on retainer for data breaches.

Information sharing

17 | Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

It is considered best practice to share information on cybersecurity threats, although this usually occurs after the threat has been properly resolved. You can share this information informally, for example through social media, or more formally on a voluntary basis to Action Fraud or the NCSC.

18 | How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The UK government's Strategy sets out an aim for the UK to establish itself as a global cyberpower, which includes strengthening the UK cyber ecosystem between government, academia and industry. The Strategy intends to build on the existing relationships between NSCS and industry stakeholders, most notably the regional cyber clusters recently formalised by the UK Cyber Cluster Collaboration.

Industry experts have also organised to help direct the UK technology sector. In particular, techUK (the UK's technology trade association) brings together organisations to enhance government collaboration and accelerate innovation. techUK has over 800 members across the UK, from sector leaders, such as Amazon and DeepMind, to law firms and emerging start-ups.

Insurance

19 | Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Insurance for cybersecurity breaches is available in the jurisdiction and has become more prevalent and available in the past five years, although the cyber insurance market has hardened significantly over the past year. Previously, insureds that suffered cyberattacks or were involved in cyber incidents would try to claim under their existing commercial insurance policies (such as, for example, those relating to property or commercial risks). While some of these 'silent' cyber risks could attach, many would not fall within cover. This state of affairs helped drive the 'affirmative' cyber insurance marketplace forward.

ENFORCEMENT

Regulation

20 | Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

A number of authorities share this responsibility. The National Cyber Crime Unit (which operates within the National Crime Agency) is responsible for responding to the most critical cyber incidents and also pursues longer-term activity against cyber criminals. The Information Commissioner's Office (ICO) enforces cybersecurity rules where they involve personal data (through the UK GDPR and Data Protection Act 2018), and enforces the NIS Regulations 2018. Industry-specific regulators (eg, the Financial Conduct Authority (FCA)) may enforce cybersecurity rules where a breach falls within their jurisdiction. Criminal prosecutions are (with some limited exceptions) carried out by the Crown Prosecution Service.

21 | Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Authorities have relatively wide-ranging powers to monitor compliance, conduct investigations and support prosecutions. The ICO has statutory powers as set out in the DPA 2018 (Parts 5 and 6). Among other things, it is empowered to conduct compliance assessments, issue information requests, enter premises, call for documents and interview staff. It is a criminal offence to obstruct a person executing an ICO warrant. Sector-specific regulators have certain similar powers, which vary between regulators and are provided for by statute (eg, the FCA).

Where criminal proceedings are on foot or in contemplation, the power of authorities to monitor and investigate are the same as those for criminal investigations generally.

22 | What are the most common enforcement issues and how have regulators and the private sector addressed them?

According to the National Cyber Security Centre (NCSC), ransomware became the most significant cyber threat facing the UK in 2021. In addition, the UK government's Strategy makes clear that ransomware attacks continue to become more sophisticated and damaging. The government's *Cyber Security Breaches Survey (2021)* also highlights the increased risk level (due to the effects of the pandemic), and that businesses are finding it harder to administer cybersecurity measures than ever before. This reality, especially when coupled with increased enforcement actions, means that cybersecurity is likely to be an ongoing issue for the private sector and beyond.

In the UK, many will recall the ICO fining Ticketmaster £1.25 million in November 2020 following a data breach in 2018 that potentially compromised data of 9.4 million customers. While regulatory enforcement concluded in 2020, the separate private group action against Ticketmaster continued until February 2022, when it reportedly reached a confidential settlement.

The attack on Microsoft's Exchange servers, which was made public by the firm in March 2021, has not yet resulted in enforcement action by the ICO or otherwise. It remains to be seen whether direct action will be taken by regulators in response, although the recent increase in enforcement activity would suggest that an announcement is imminent.

23 | What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

The UK GDPR places a legal obligation on all organisations to report cybersecurity breaches to the ICO within 72 hours of becoming aware of any given breach. The threshold for notification to the ICO will be met if the breach leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A notification to the ICO is not required where the business can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the business who is subject to the breach must also inform those affected individuals without 'undue delay', and, in practice, this should be done as soon as possible.

While the obligations under the UK GDPR have general application, additional notification obligations may arise depending on the nature of the organisation. For example, UK trust service providers must notify the ICO of a security breach that may include a personal data breach within 24 hours under the Electronic Identification and Trust Services (eIDAS) Regulation.

Penalties

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Cybersecurity law in the jurisdiction has not been centrally codified and instead is based on a legal framework comprised of a number of statutory enactments. It is therefore difficult to discuss penalties for regulatory breaches in the round, as they apply to all businesses.

By way of an example, however, the Network and Information Systems Regulations 2018 impose obligations on operators of essential services and relevant digital service providers. The former operate services that are deemed critical to the economy such as energy, water and transport. The latter operate (among others) online marketplaces and provide cloud computing services. The regulations require these entities to have sufficient security systems in place, and allow a competent authority (the ICO) to impose penalties for breaches of its provisions.

Where, for example, there has been a material contravention of the regulations, which is deemed to have caused (or could cause) an incident resulting in the disruption of service for a significant period of time, penalties of up to £8.5 million are capable of being imposed. If the disruption results in an immediate threat to life or a significant adverse impact on the economy, the penalty could be up to £17 million.

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Again, the absence of a centrally codified cybersecurity law makes it difficult to discuss penalties for regulatory breaches in the round, as they apply to all businesses.

Most of the relevant regulations impose obligations to report either threats or breaches and in doing so, give competent authorities the power to issue penalties (usually in the form of enforcement notices). By way of an example, the Network and Information Systems Regulations 2018 require incidents to be reported without undue delay. If, however, a failure to do so amounts to a 'material contravention', the penalty could, in theory, be up to £17 million in certain circumstances. Where personal data is involved, the Data Protection Act 2018 and the UK GDPR will also be relevant.

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

The GDPR gives you a right to claim compensation if you have suffered damage as a result of breach of data protection laws. 'Damage' includes material and non-material damage, meaning financial loss or suffering distress (an arguably low bar). In the first instance you should contact the individual or company who held your data at the time of the breach; they may agree to pay you without further action. If they don't, you might consider bringing formal proceedings (although you should take independent legal advice before doing so).

More recently we have seen a rise in group action claims for mass data breaches, although we expect this trend to plateau following the recent supreme court decision in *Lloyd v Google*, which refused a large-scale representative action (similar to US class actions).

THREAT DETECTION AND REPORTING

Policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

UK legislation does not mandate specific policies or procedures in this respect. The security principle set out in the UK GDPR requires organisations to process personal data securely by implementing appropriate technical and organisational measures. Similarly, the Network and Information Systems Regulations (NISR) require operators of essential services (OESs) and relevant digital service providers (RDSPs) to undertake measures to manage the risks posed to the security of their networks. Under the UK GDPR and the NISR, organisations should assess the security risk associated with their own operations and implement appropriate controls, which could be in the form of organisational policies, physical and technical measures and/or conducting risk analysis.

Organisations regulated by the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) will need to comply with the data security obligations set out in the Financial Services and Markets Act and are required to have in place adequate systems and controls to monitor, detect and prevent financial crime.

28 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Under the UK GDPR organisations are required to record all personal data breaches, regardless of whether they are reported to a regulator. There is no specific rule on format or timing for retaining the records, although the record must contain the facts relating to each data breach, its effect and the remedial action taken.

Under the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), the Information Commissioner's Office (ICO) requires that communications network and service providers keep a log of any personal data breaches, and that they submit this to the ICO on a monthly basis. The log should contain the facts of the breach, the consequences and any remedial action taken.

Under the NISR, regulated entities must maintain records evidencing the appropriate and proportionate technical and organisational measures taken to manage risks to their systems. The NISR do not prescribe any format or retention period for these records. Records should be accurate and accessible to the competent authority.

29 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

For breaches that compromise network security, the NISR require OESs and RDSPs to notify the ICO of security incidents without undue delay. The government is consulting on changes to the NISR which would require enhanced cyber incident reporting to other regulators, such as Ofcom and Ofgem. The government also proposes a requirement to notify regulators of all incidents that pose a significant risk to resilience and security, not just those that directly impact services.

In relation to cybersecurity breaches that involve personal data, the UK GDPR and the DPA 2018 requires data controllers to notify the ICO without undue delay, and no later than 72 hours after becoming aware of the incident, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. The notification must provide details of (1) the nature of the breach; (2) the organisation's Data Protection Officer (if relevant); (3) the likely consequences of the breach; and (4) the measures taken, or proposed to be taken, to deal with or mitigate any possible adverse effects.

The PECR require telecoms and internet service providers to notify the ICO if a personal data breach occurs within 24 hours of becoming aware of the facts of the breach. The notification must include the name of the service provider, circumstances of the breach, nature and content of the personal data and the technical and organisational measures applied to the affected personal data.

The ICO website provides links for the reporting of incidents under the UK GDPR, PECR, and NISR.

The FCA also requires regulated organisations to notify the FCA and PRA in the case of a data security breach.

Time frames

30 | What is the timeline for reporting to the authorities?

The UK GDPR places a legal obligation on all organisations to report cybersecurity breaches to the ICO within 72 hours of becoming aware of any given breach. The threshold for notification to the ICO will be met if the breach leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A notification to the ICO will not be required where the business can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the business that is subject to the breach must inform those affected individuals without 'undue delay'. In practice, the notification to the data subject will be required as soon as possible provided the breach is sufficiently severe to be considered high risk.

While the obligations under the GDPR have general application, additional notification obligations may arise depending on the nature of the organisation. For example, UK trust service providers must notify the ICO of a security breach that may include a personal data breach within 24 hours under the eIDAS Regulation.

The NISR also impose reporting standards on these organisations in essential services, with mandatory notification to the relevant authority within 72 hours of becoming aware of an incident occurring.

Reporting

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

There are no generally applicable requirements to reports threats or breaches to industry, customers or the general public.

In relation to cybersecurity breaches that involve personal data, the UK GDPR requires data controllers to inform affected individuals about breaches that are likely to result in a high risk to their rights, without undue delay, after becoming aware of the incident. The communication must provide details of (1) the organisation's data protection officer (if relevant); (2) the likely consequences of the breach; and (3) the measures taken, or proposed to be taken, to deal with or mitigate any possible adverse effects.

UPDATE AND TRENDS

Key developments of the past year

32 | What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Cybersecurity affects all internet-enabled businesses, but imposing the same regulations on all market participants is not practical. To date, UK regulations have focused on critical service providers, with the National Cyber Security Centre issuing guidance to sectors of the economy such as the self-employed and small and medium-sized enterprises.

Cybersecurity regulations must also allow for flexibility and be technology-agnostic to enable emerging threats to be countered. It is in this spirit that the UK government is consulting on changes to the Network and Information Systems Regulations 2018 (NISR) to create a process for the government to designate unregulated organisations as being 'critical' and therefore subject to the NISR's requirements.

The government is currently consulting on changing the scope of the NISR to encompass a broader range of service providers and incident types, among other developments.

* *The authors would like to thank Felix Zimmermann, Rachel Mahoney, Ryan Williams and Martin Murphy for their contribution to the chapter.*

simmons+simmons

Robert Allen
robert.allen@simmons-simmons.com

Lawrence Brown
lawrence.brown@simmons-simmons.com

Neil Westwood
neil.westwood@simmons-simmons.com

Russell Cowie
russell.cowie@simmons-simmons.com

Emily May
emily.may@simmons-simmons.com

Citypoint
1 Ropemaker Street
London, EC2Y 9SS
United Kingdom
Tel: +44 20 7628 2020
Fax: +44 20 7628 2070
www.simmons-simmons.com

simmons+simmons

Our team provides a business-focused and pragmatic approach.

Our international data, privacy and cybersecurity practice spans the globe advising within the Asset Management & Investment Funds, Financial Institutions, TMT and Healthcare & Life Sciences sectors.

Our lawyers advise on the full suite of data and cybersecurity issues – from implementing preventative measures and regulatory requirements through to data breach response and full-scale litigation.

simmons-simmons.com

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Digital Business
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

ISBN 978-1-83862-941-0