
CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2023

Definitive global law guides offering
comparative analysis from top-ranked lawyers

UK: Law & Practice

William Long, Eleanor Dodding,
João Diogo Quartilho and
Subhalakshmi Kumar
Sidley Austin LLP

UK: Trends and Developments

William Long, Eleanor Dodding,
João Diogo Quartilho and
Subhalakshmi Kumar
Sidley Austin LLP

Law and Practice

Contributed by:

William Long, Eleanor Dodding,
João Diogo Quartilho and Subhalakshmi Kumar
Sidley Austin LLP see p.22



Contents

1. Basic National Regime	p.4	4. Key Affirmative Security Requirements	p.15
1.1 Laws	p.4	4.1 Personal Data	p.15
1.2 Regulators	p.5	4.2 Material Business Data and Material Non-public Information	p.15
1.3 Administration and Enforcement Process	p.6	4.3 Critical Infrastructure, Networks, Systems	p.15
1.4 Multilateral and Subnational Issues	p.8	4.4 Denial of Service Attacks	p.15
1.5 Information Sharing Organisations and Government Cybersecurity Assistance	p.8	4.5 Internet of Things (IoT), Software, Supply Chain, Other Data or Systems	p.15
1.6 System Characteristics	p.8	4.6 Ransomware	p.15
1.7 Key Developments	p.9	5. Data Breach or Cybersecurity Event Reporting and Notification	p.15
1.8 Significant Pending Changes, Hot Topics and Issues	p.10	5.1 Definition of Data Security Incident, Breach or Cybersecurity Event	p.15
2. Key Laws and Regulators at National and Subnational Levels	p.11	5.2 Data Elements Covered	p.17
2.1 Key Laws	p.11	5.3 Systems Covered	p.17
2.2 Regulators	p.11	5.4 Security Requirements for Medical Devices	p.17
2.3 Over-Arching Cybersecurity Agency	p.11	5.5 Security Requirements for Industrial Control Systems (and SCADA)	p.18
2.4 Data Protection Authorities or Privacy Regulators	p.11	5.6 Security Requirements for IoT	p.18
2.5 Financial or Other Sectoral Regulators	p.11	5.7 Requirements for Secure Software Development	p.18
2.6 Other Relevant Regulators and Agencies	p.12	5.8 Reporting Triggers	p.18
3. Key Frameworks	p.12	5.9 "Risk of Harm" Thresholds or Standards	p.18
3.1 De Jure or De Facto Standards	p.12	6. Ability to Monitor Networks for Cybersecurity	p.19
3.2 Consensus or Commonly Applied Framework	p.13	6.1 Cybersecurity Defensive Measures	p.19
3.3 Legal Requirements and Specific Required Security Practices	p.13	6.2 Intersection of Cybersecurity and Privacy or Data Protection	p.19
3.4 Key Multinational Relationships	p.14		

7. Cyberthreat Information Sharing Arrangements	p.19
7.1 Required or Authorised Sharing of Cybersecurity Information	p.19
7.2 Voluntary Information Sharing Opportunities	p.19
8. Significant Cybersecurity and Data Breach Regulatory Enforcement and Litigation	p.19
8.1 Regulatory Enforcement or Litigation	p.19
8.2 Significant Audits, Investigations or Penalties	p.20
8.3 Applicable Legal Standards	p.20
8.4 Significant Private Litigation	p.20
8.5 Class Actions	p.20
9. Cybersecurity Governance, Assessment and Resiliency	p.20
9.1 Corporate Governance Requirements	p.20
10. Due Diligence	p.20
10.1 Processes and Issues	p.20
10.2 Public Disclosure	p.21
11. Insurance and Other Cybersecurity Issues	p.21
11.1 Further Considerations Regarding Cybersecurity Regulation	p.21

1. Basic National Regime

1.1 Laws

The UK has a well-developed – and growing – network of civil and criminal laws relating to cybersecurity, contained in UK legislation, companion rules made under such legislation, decisions of UK courts and a steady stream of regulatory guidance from UK regulators.

Key cybersecurity requirements imposed on organisations in the UK, or on organisations established outside of the UK but who are processing personal data of individuals located in the UK, are derived from the EU General Data Protection Regulation (EU GDPR). Following the UK's departure from the EU under the terms of the EU (Withdrawal Agreement) Act 2020 on 31 January 2020, the UK government adopted the EU GDPR into UK law as the "UK GDPR", which took effect in UK law following the end of the Brexit Transition Period on 31 December 2020.

The UK GDPR and the UK Data Protection Act 2018 (DPA), as amended to supplement the UK GDPR in UK law, applies to the security of "personal data" under the UK GDPR (eg, any information relating to an identified or identifiable individual who can be identified, directly or indirectly by reference to an identifier such as a name, an identification number, location data or an online identifier). As such, only those cybersecurity incidents impacting personal data will be regulated by the UK GDPR (see also **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**). The UK GDPR requires organisations to maintain "appropriate" technical and organisational security measures and to comply with certain notification obligations when "personal data breaches" occur. The DPA also allows for criminal prosecutions to be brought for certain cybersecurity-related breaches.

Secondly, Network and Information Systems Regulations (NIS Regulations). The NIS Regulations apply to two categories of key infrastructure operators, namely "operators of essential services" (OESs) and "relevant digital service providers" (RDSPs). Like the UK GDPR, the NIS Regulations require organisations that are subject to them to implement certain cybersecurity measures and to provide notices of certain cybersecurity incidents that affect such organisations. In November 2022, the UK government confirmed that legislative changes resulting from a public consultation in January 2022 would be made to boost security standards and to increase reporting of serious cyber-incidents to reduce the risk of such attacks causing disruption. Please see **1.7 Key Developments** for additional information on the development of the NIS Regulations.

Thirdly, the Product Security and Telecommunications Infrastructure Act 2022 (PSTI). PSTI requires manufacturers, importers and distributors of UK consumer connected products to meet certain cybersecurity standards. This includes requirements to follow more stringent security requirements (which will be specifically legislated by the UK Secretary of State), to investigate any compliance failures and take remediation action, as well notify relevant authorities and other third parties about such compliance failures. Please see **1.7 Key Developments** for additional information on the obligations under the PSTI.

Fourthly, the Computer Misuse Act 1990 (CMA). The CMA is the UK's primary legislation with respect to criminalising unauthorised access to computers and other IT systems. It contains a number of cybersecurity-related offences. A key offence under the CMA (Section 1) is where a defendant obtains "unauthorised access" to a

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

computer: the defendant causes a “computer to perform any function with intent to secure access to any program or data held in any computer” or “to enable such access to be secured” where such access is “unauthorised” and this is known to the defendant at the relevant time.

Fifthly, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), the EU Notification Regulations 611/2013 (the Notification Regulation), and the Communications Act 2003 (CA 2003). These laws contain cybersecurity obligations applicable primarily to electronic communications networks and service operations (such as telecommunications systems operators).

There are also sector-specific laws that contain cybersecurity obligations, for example, FCA rules (applicable to organisations that the FCA regulates), Payment Services Regulations 2017 (PSR) (which transposes the Second Payment Services Directive into UK law, and applies to payment service providers), and the Official Secrets Act 1989 (OSA, applicable to certain official government information). Similarly, the Investigatory Powers Act 2016 (IPA) and the Regulation of Investigatory Powers Act 2000 (RIPA) regulate electronic surveillance and interception in the UK and contain associated safeguards.

These laws are increasingly being enforced by UK governmental authorities – including the Information Commissioner’s Office (ICO) and sector-specific regulators such as the Financial Conduct Authority (FCA) – and private individuals and organisations. Regulators are also increasingly collaborating on cybersecurity enforcement; examples include the ICO teaming up with the Competition and Markets Authority (CMA), the Office of Communications (Ofcom) and the

Financial Conduct Authority (FCA) to form the Digital Regulation Cooperation Forum (DRCF).

In addition to legislation, English “common law” contains rules that are relevant to cybersecurity: there is a legal and ethical duty of confidence where information is shared in confidence and must not be disclosed without legal authority. The duty applies to information not already in the public domain and is subject to a number of exceptions, including where disclosure:

- has been consented to by the discloser; or
- is required by law.

The FCA rules, PSR, OSA, IPA, RIPA and other sector-specific or specialised laws or the common law duty of confidence are not further considered in this chapter.

1.2 Regulators

There are different UK regulators for each of the key UK cybersecurity legislations under consideration.

UK GDPR and DPA

In the UK, the ICO is responsible for monitoring the application of the UK GDPR and the DPA and taking enforcement action against organisations for non-compliance with such legislation, including investigating personal data breaches and inadequate security measures. The ICO may initiate an investigation on its own accord or on the basis of a complaint submitted by (for example) a private individual or organisation. The ICO also has the power to conduct both off-site and on-site audits.

NIS Regulations

With respect to the NIS Regulation, the “competent authority” is determined on an industry-by industry basis, through the Department for Digi-

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

tal, Culture, Media & Sport (DCMS), which oversees the implementation of the NIS Regulations across the UK. For example, for OESs in the oil sector, the competent authority in England, Scotland and Wales is the Secretary of State for Business, Energy and Industrial Strategy, while in Northern Ireland it is the Department of Finance. The ICO is the competent authority for RDSPs. Competent authorities may be reactive or proactive in terms of the incidents they choose to investigate and they are supported by the National Cyber Security Centre (NCSC) who offer technical advice, except in healthcare where this support is offered by NHS Digital. Certain organisations are also subject to regular compliance audits from their relevant competent authority – failing these audits can lead to fines of up to GBP17 million.

PECR and CA 2003

In regard to PECR, the ICO may audit the compliance of service providers pursuant to Regulation 5A of PECR. Notifiable personal data breaches under Regulation 5A of PECR must be reported to the ICO. The ICO is, in turn, responsible for investigating the breach and taking any subsequent enforcement action (see also **1.3 Administration and Enforcement Process**). However, with respect to the CA 2003, which is a companion legislation to PECR, Ofcom is the primary regulator. Pursuant to Section 105C of the CA 2003, Ofcom may carry out an audit of the security measures taken by a network provider or a service provider under Section 105A. Notifiable security breaches under Section 105 of CA 2003 must be reported to Ofcom, which is, in turn, responsible for investigating the breach and taking any subsequent enforcement action (see also **1.3 Administration and Enforcement Process**).

CMA

While there is no regulatory authority with oversight of the CMA per se, the provisions of the CMA are enforced by the UK Crown Prosecution Service (CPS), the public authority responsible for prosecuting the majority of criminal cases in the UK. The CPS is notified of CMA investigations and potential offences by the police and other investigative organisations in England and Wales. As noted above, the DPA is enforced by the ICO and prosecutions under the DPA can only be brought by the ICO, or by or with the consent of the Director of Public Prosecutions (DPP).

1.3 Administration and Enforcement Process

The administration and enforcement process varies on a UK cybersecurity legislation-by-legislation basis. Commentary on the enforcement of certain key UK cybersecurity legislation is provided below.

UK GDPR and DPA

At present, the UK GDPR and the DPA continue to be enforced by the ICO, including with respect to cybersecurity matters – but only to the extent they impact personal data. The ICO is required to adhere to specific procedures before undertaking enforcement action. For example, before imposing an administrative fine on an organisation for:

- breaching the integrity and confidentiality principle;
- inadequate security measures; or
- failing to report a personal data breach to the ICO or affected data subjects.

Where applicable, the ICO is required under Section 149 of the DPA to first issue the organisation with a written “enforcement notice”, which

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

requires the organisation to take steps specified in the notice and/or refrain from taking steps specified in the notice.

If the ICO is of the view that the organisation has failed to comply with the enforcement notice, the ICO will then issue a written notice (“penalty notice”) imposing a monetary penalty on the organisation of up to the greater of 4% of annual worldwide turnover or GBP17.5 million. When determining the monetary penalty amount, the ICO will consider a number of aggravating or mitigating factors. These factors include the nature, gravity and duration of the infringement – for example, personal data breach or inadequate security measures, and the intentional or negligent character of the infringement.

In determining whether to undertake a criminal prosecution under the DPA, the ICO must reference the Code for Crown Prosecutors and the ICO’s own prosecution policy. While the ICO has a number of enforcement tools available to it (including providing a caution to offending organisations), the ICO’s Prosecution Policy Statement requires the ICO to consider aggravating factors to bring a prosecution instead of a caution. These include the accused breaching the law for financial gain, abusing a position of trust, or damage or distress being caused to data subjects.

The maximum penalty for criminal offences under the DPA is an unlimited fine. Imprisonment is not available for conviction under any of the DPA offences. Defendants are entitled to normal rights of appeal against a conviction or sentence in the legal system.

PECR, Notification Regulation and CA 2003

The ICO’s guidance on notification of PECR security breaches provides that, upon receipt of

a notification from a service provider, the ICO will consider the information provided in the notice to assess whether the service provider is complying with its obligations under PECR. The ICO further states that it will inform the service provider of next steps within two weeks of their notification. Pursuant to Regulation 5C of PECR, if a service provider fails to comply with the notification requirements of Regulation 5A, the ICO may issue a fixed monetary penalty notice of GBP1,000 against the service provider.

Before serving the enforcement notice, the ICO must serve the service provider with a notice of intent. A service provider may discharge liability for the fixed monetary penalty if such service provider pays GBP800 to the ICO within 21 days of receipt of the notice of intent. A service provider can also appeal the issuance by the ICO of the fixed monetary penalty notice to the First-tier Tribunal (Information Rights). The ICO also has the power under PECR to issue enforcement notices for breach of the provisions of PECR of up to a maximum of GBP500,000. However, the UK Data Protection and Digital Information Bill is proposing to increase fines for infringement to align with UK GDPR levels.

Under Section 105E, Ofcom has the power to issue penalties of up to GBP2 million where appropriate and proportionate.

CMA

There are a number of offences under the CMA. Section 1 is hereby considered, as noted previously, an offence under Section 1 is committed if there is “unauthorised” access to a computer system. A Section 1 CMA offence is triable both summarily in the magistrates’ courts and on indictment in the Crown Court. Offences committed under Section 1 CMA carry up to two years’ imprisonment or an unlimited fine, or

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

both, on indictment. On summary conviction, the maximum sentence is 12 months' imprisonment or a fine, or both. In addition, a serious crime prevention order can be made against an individual or an organisation in relation to a breach of the CMA. Defendants are entitled to normal rights of appeal against a conviction or sentence in the legal system.

In determining whether to bring a prosecution under the CMA, the CPS must be satisfied that there is enough evidence to provide a "realistic prospect of conviction" against each defendant and that the public interest factors tending against prosecution outweigh those tending in favour, as set out in the Code for Crown Prosecutors 2018, which sets out the general principles which must be followed when the CPS makes a decision on cases. While there are no official guidelines for sentencing offences under the CMA, judges and magistrates will have to follow the Sentencing Council's General guideline which applies to all offences without specific sentencing guidelines.

1.4 Multilateral and Subnational Issues

The UK GDPR and the DPA apply to:

- all organisations established in the four countries of the UK (ie, England, Northern Ireland, Scotland and Wales); and
- organisations not established in the UK processing personal data of data subjects in the UK to offer goods or services or to monitor their behaviour.

In turn, the ICO regulates the UK GDPR and the DPA across the UK.

While the CMA primarily applies to offences committed within the UK, it allows for prosecutions to be brought in the UK where some or all

of the offending acts were committed outside the UK – reflecting the trans-border nature of many cybersecurity-related offences. For example, Section 1 of the CMA can apply to offending acts committed outside the UK and can, as a result, be prosecuted in the UK where there is "at least one significant link with the domestic jurisdiction". A significant link can include where:

- the accused is in a relevant country of the UK (England, Wales, Scotland and Northern Ireland) at the time of the offence;
- the target of the CMA offence is in a relevant country of the UK; or
- the technological activity which has facilitated the offending may have passed through a server based in a relevant country of the UK.

1.5 Information Sharing Organisations and Government Cybersecurity Assistance

Please see 7. Cyberthreat Information Sharing Arrangements.

1.6 System Characteristics

The UK cybersecurity legal system is well developed and is similar to the legal systems across the EEA (rather than the USA). Since 2018, the enforcement of cybersecurity rules in the UK has increased, particularly by the ICO. Notably, in October 2020 the ICO fined British Airways GBP20 million following a cyber-attack resulting in user traffic to the British Airways website and mobile application being diverted to a fraudulent website which allegedly led to the compromise of the personal data of over 400,000 customers.

Also in October 2020, the ICO fined Marriott International (Marriott) GBP18.4 million for alleged failures relating to cybersecurity in the context of an acquisition.

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

More recently, in October 2022, the ICO fined a construction company GBP4.4 million for failure to adopt appropriate security measures to prevent a cyber-attack. The cyber-attack was the result of a phishing email received by an Interserve employee which resulted in the installation of malware onto another employee's workstation. The ICO considered that the malware was not thoroughly investigated despite the company's anti-virus software providing an alert and quarantining the malware. As a result, the malware compromised 283 systems and 16 accounts. The malware also encrypted the personal data of 113,000 current and former employees.

The UK government is also expected to overhaul its ability to assist and promote cybersecurity through its government cybersecurity strategy for 2022-30. There is to be a focus on government functions, including:

- the establishment of the Government Cyber Coordination Centre (GCCC);
- the adoption of the Cyber Assessment Framework (CAF); and
- dedicating more resources into tackling ransomware.

1.7 Key Developments

The key developments in the UK from a cybersecurity perspective in the past 12 months include confirmation from the UK government that it will amend the NIS Regulations as a result of a public consultation by the UK government on proposals for legislation to improve the UK's cyber-resilience. The consultation included proposals for the expansion of the scope of application of the NIS Regulations and new discretionary powers for the UK government to expand the scope and covered entities of the NIS regulations to manage IT risks. In particular, the planned

amendments to NIS Regulations will include the following.

- Managed service providers (MSPs) will be included in the list of "relevant digital service providers".
- A new, two-tier supervisory regime will be introduced, with a proactive supervisory regime applying for the most critical digital service providers and the existing, reactive supervisory regime continuing to apply to the remaining digital service providers. The plans indicate that ICO would be the competent regulator for the two regulatory regimes.
- The UK government will receive delegated powers to expand the scope of the NIS Regulations without Parliament's consent and may inclusively designate entities as "critical (sector) dependencies" to ensure that entities such as relevant IT supply chain stakeholders that would not be covered by the NIS regulations are brought into its scope.
- Expanding incident reporting requirements to include "any incident which has a significant impact on the availability, integrity, or confidentiality of networks and information systems, and that could cause, or threaten to cause, substantial disruption to the service".

There is currently no concrete timeline for the planned amendments.

Secondly, the PSTI came into force on 6 December 2022. Under this new act, manufacturers (the person responsible for manufacturing a product, designing a product or otherwise marketing the product under their own name or trade mark) of "UK consumer connectable products" are required to comply with new obligations to manage cyber security risk of connected products made available in the UK. Similar obligations will also apply to importers and distributors:

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

- duty to comply with security requirements as defined by the Secretary of State (see **5.6 Security Requirements to IoT**);
- duty to investigate and take action in relation to compliance failures – which may include preventing the product from being made available in the UK and/or remedying the compliance failure and notifying enforcement authorities, other manufacturers, importers and distributors; and
- duty to maintain records for a minimum of ten years – these records may be requested by the Secretary of State in the course of investigating and enforcing the legislation.

The new regime will be overseen by the Secretary of State that will have the power to levy GDPR-style fines of GBP10 million or 4% of their annual revenue, as well as up to GBP20,000 a day in the case of an ongoing contravention.

Thirdly, on 8 July 2022, the ICO and the National Cyber Security Centre (NCSC) sent a joint letter to the Law Society setting out their policy position against paying ransoms in the context of ransomware attacks. The regulators consider that paying hackers ransoms provides no guarantees that the malicious actors will provide the decryption keys and does not ensure the safe return and/or erasure of the exfiltrated data. Additionally, the ICO clarified that it will not take the payment of ransoms into account as mitigating factor when considering the type or scale of a GDPR enforcement action. The ICO has also published a revised version of its Ransomware and data protection compliance guidance on its website.

1.8 Significant Pending Changes, Hot Topics and Issues

There are three key UK cybersecurity matters on the horizon over the next 12 months, as detailed below.

Firstly, the DCMS is continuing to work on cybersecurity legislative initiatives, such as the stringent security requirements that will be imposed under the PTSI and the results of its public consultation regarding the development of standards and pathways for cybersecurity professionals.

Secondly, the UK government has also concluded its Cyber Security Regulation and Incentives Review, which stated that cybersecurity advice and guidance by the UK government was not reaching a sufficient audience and that the government needs to improve its messaging efforts. The review set out wide-ranging new actions to be taken by the UK government such as:

- promoting the Cyber Essentials as a fundamental cybersecurity certification scheme;
- providing more specific guidance on supplier assurance for procurers, and to establish a cybersecurity baseline for critical providers of digital technology services such as MSPs; and
- proposing to strengthen the UK cyber legislation (please see comments at **1.1 Key Developments**).

Thirdly, the UK government is making moves to amend the CMA, as for many years commentators have stated that the CMA has failed to keep pace with the cybersecurity landscape. The Criminal Law Reform Now Network produced a short comparative report on Reforming the Computer Misuse Act, which highlights reforms needed across the landscape of cyber-hacking

regulation. This includes issues with the ambiguity around the meaning of “authorisation” and its subsequent impact on cybersecurity professionals, as well as highlighting issues with the current jurisdictional scope of the CMA, given the international nature of many cybersecurity incidents. The UK government held a consultation on CMA reform in 2021, and in April 2022 future reforms were discussed in Parliament; however, the UK government is yet to make public any formal proposal to reform the CMA.

2. Key Laws and Regulators at National and Subnational Levels

2.1 Key Laws

Please see comments at **1.1 Laws**.

2.2 Regulators

Please see comments at **1.2 Regulators** and **1.3 Administration and Enforcement Process**.

2.3 Over-Arching Cybersecurity Agency

The UK National Cybersecurity Centre (NCSC) is the key UK cybersecurity agency, co-ordinating UK cybersecurity policy and technical standards, particularly with respect to the NIS Regulations and the UK GDPR. The NCSC acts as the national computer security incident response team (CSIRT) under the NIS Regulations and supports organisations that suffer cybersecurity incidents. It also acts as a “single point of contact” for competent authorities under the NIS Regulations. Following Brexit, the UK has forfeited its position on the EU Agency for Cybersecurity (ENISA); however, some operational co-operation continues to persist to allow for improved cybersecurity across Europe.

2.4 Data Protection Authorities or Privacy Regulators

Please see comments at **1.1 Laws**, **1.2 Regulators** and **1.3 Administration and Enforcement Process**. As a result of overlapping jurisdictions among the various cybersecurity laws, multiple regulators may exercise jurisdiction with respect to the same cybersecurity incident. For example, a major cybersecurity incident affecting an OES that results in the compromise of personal data could implicate the UK GDPR and the NIS Regulations and thereby involve notices to both the ICO and the relevant “competent authority” under the NIS Regulations. Similarly, a major cybersecurity incident affecting an FCA-regulated organisation that results in the compromise of personal data could, for example, implicate the UK GDPR and the FCA rules and thereby involve notices to both the ICO and the FCA respectively.

2.5 Financial or Other Sectoral Regulators

Please see comments at **1.1 Laws**, **1.2 Regulators** and **1.3 Administration and Enforcement Process**. Also, and by way of illustration, the FCA has demonstrated a strong focus on cybersecurity in the context of the financial services industry. This is particularly relevant in the context of:

- Principle 3 (Management and Control) of the FCA Handbook PRIN Principles for Businesses, which states that “a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems”; and
- Principle 11 (Relations with Regulators) which requires that “a firm must deal with its regulators in an open and co-operative way, and must disclose to the FCA appropriately any-

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

thing relating to the firm of which that regulator would reasonably expect notice”.

In relation to Principle 11, the FCA confirms that organisations must report material cyber-incidents. The FCA considers that an incident may be material if it:

- results in significant loss of data, or the availability or control of a firm’s IT systems;
- affects a large number of customers; and
- results in unauthorised access to, or malicious software present on, a firm’s information and communication systems.

The FCA goes on to require that where such an incident is deemed to be material:

- the FCA (and the Prudential Regulation Authority for dual-regulated firms) should be notified;
- if the incident is criminal, Action Fraud (the UK’s national fraud and cybercrime reporting centre) should be contacted; and
- where the incident is also a data breach, organisations may need to report the incident to the ICO.

The FCA also recommends that firms refer to the NCSC guidance on reporting incidents and reports should be shared on the CiSP platform; please see comments at **7.2 Voluntary Information Sharing Opportunities** for further detail on the CiSP platform. More generally, and as part of the FCA’s goal to assist firms in becoming more resilient to cyber-attacks, it recommends that firms of all sizes should develop a “security culture” and be able to identify and prioritise information assets and constantly evolve to meet new threats.

In addition, certain categories of FCA-regulated firms have additional reporting requirements. For example, payment services providers are required to report major operational and security incidents pursuant to the PSR.

2.6 Other Relevant Regulators and Agencies

Please see comments at **1.1 Laws**, **1.2 Regulators**, **1.3 Administration and Enforcement Process** and **2.4 Data Protection Authorities or Privacy Regulators**.

3. Key Frameworks

3.1 De Jure or De Facto Standards

There are numerous cybersecurity frameworks that are expressly or implicitly recognised by UK cybersecurity regulators. For example, the ICO recommends that organisations review the UK Cyber Essentials scheme (a UK government and industry-backed scheme), which provides basic guidance to organisations on how to prevent and limit the impact of cyber-attacks.

Similarly, Ofcom repeatedly references the International Standard for Organization (ISO) standards in its Guidance on Security Requirements. In addition, Ofcom comments that the controls in the UK’s Cyber Essentials scheme should be implemented and exceeded; according to Ofcom, obtaining the Cyber Essentials Plus certification is “a powerful way to demonstrate this”. Regarding the NIS Regulations, the NCSC has published 14 cybersecurity and resilience principles that provide guidance in the form of the Cyber Assessment Framework (CAF). The CAF is particularly relevant to OESs that are subject to the NIS Regulations.

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

Lastly, the most used account and payments data security standard, the PCI Data Security Standard (PCI DSS), was revised and the version 4.0 was published on 31 March 2022.

3.2 Consensus or Commonly Applied Framework

Please see comments in 3.1 **De Jure or De Facto Standards** and 3.3 **Legal Requirements and Specific Required Security Practices**.

3.3 Legal Requirements and Specific Required Security Practices

UK GDPR

The UK GDPR requires that controllers and processors implement “appropriate” technical and organisational security measures. When adopting such measures, the UK GDPR requires organisations to take into account the state-of-the-art, costs of implementation and the nature, scope, context, purposes of the processing of personal data and risks of such processing to the data subject’s rights (eg, from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed by the organisation).

The UK GDPR itself sets out examples of “appropriate” security measures, namely:

- pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical

and organisational measures for ensuring the security of personal data processing.

Importantly, according to the ICO, there is no “one-size-fits-all” approach to “appropriate” security. The level of appropriateness depends on each organisation’s processing of personal data – for example, the nature of the organisation’s computer systems, the number of personnel with access to the personal data being processed and whether any personal data is held by a vendor acting on the organisation’s behalf. The ICO recommends that, before taking a view on what is “appropriate”, organisations should assess the level of risk by reviewing the type of personal data held, whether it is sensitive or confidential and the damage caused to data subjects if compromised (eg, identity fraud).

In addition, when considering what cybersecurity measures to adopt, the ICO recommends that organisations consider:

- system security – security of the organisation’s network and information systems, particularly systems that process personal data;
- data security – security of the personal data held in the organisation’s systems (eg, ensuring appropriate access controls are in place within the organisation);
- actively managing software vulnerabilities, including using in-support software and the application of software update policies (patching), and taking other mitigating steps, where patches cannot be applied;
- online security – website and mobile application security; and
- device security – considering information security policies for bring-your-own devices, where offered by the organisation.

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

NIS Regulations

The NIS Regulations require that OESs and RDSPs adopt “appropriate and proportionate” technical and organisational security measures and “appropriate” measures to prevent and minimise the impact of incidents affecting those systems (taking into account the state-of-the-art) to ensure the continuity of the essential services that the OES provides. While serious incidents must be reported under the NIS Regulations, the ICO has also explained that software vulnerabilities – ie, weaknesses in a system that can be exploited by an attacker – may also need to be reported, as per the “Additional information” required in the ICO’s NIS Reporting form. As explained in **1.1 Laws**, the UK government is also consulting on updates to the NIS Regulations.

Product Security and Telecommunications Infrastructure Act 2022

As detailed in **1.7 Key Developments** and **1.8 Significant Pending Changes, Hot Topics and Issues** and **5.6 Security Requirements for IoT** the security requirements under the PSTI imposed on manufacturers, importers and distributors of UK consumer connected products made available in the UK are yet to be published by the Secretary of State.

PECR and CA 2003

Regulation 5(1A) of PECR requires service providers to:

- restrict access to personal data to only authorised personnel;
- protect personal data against “accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure”; and
- implement a security policy with respect to the processing of personal data.

Service providers are also required to retain a log of the personal data breaches pursuant to Regulation 5A(8) of PECR.

Guidance on Security Requirements published by Ofcom in relation to the CA 2003 states that “clear lines of accountability (must be established), up to and including Board or company director level, and sufficient technical capability to ensure that potential risks are identified and appropriately managed”. The guidance further states that “a level of internal security expertise, capacity, and appropriate accountability mechanisms, sufficient to provide proper management of (security risks)” must be maintained. The guidance also references the following:

- the importance of internal risk assessments;
- the need for sufficient oversight of networks and services to enable fast identification of significant security incidents;
- a requirement to put in place security measures which exceed those in the Cyber Essentials scheme; and
- the importance of intelligence-led vulnerability testing to manage cyber-risks.

3.4 Key Multinational Relationships

A number of key UK cybersecurity regulators or organisations – eg, the ICO and NCSC – work closely with their counterparts in the EEA, such as other data privacy authorities that comprise the European Data Protection Board (with respect to the ICO) and ENISA (with respect to the NCSC). In relation to relationships with other EEA data privacy authorities, the ICO, in particular, has mutual assistance memoranda of understanding with the US Federal Trade Commission, the federal Privacy Commissioner of Canada New Zealand’s Office of the Privacy Commissioner (OPC) and Department of Internal

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

Affairs, and the National Privacy Commission of the Philippines.

In addition, sector-specific regulators also work closely with their counterparts within the EEA and elsewhere. By way of illustration, the FCA has a close relationship with the SEC. While the relationship is not cybersecurity-specific, cybersecurity forms part of the regulators' general financial regulatory co-operation. The FCA has also confirmed that it continues to work with governments and other regulators, nationally and internationally, on cybersecurity issues.

4. Key Affirmative Security Requirements

4.1 Personal Data

Please see comments under **1.1 Laws, 1.2 Regulators and 1.3 Administration and Enforcement Process**, as well as **5. Data Breach Reporting and Notification**.

4.2 Material Business Data and Material Non-public Information

Please see comments under **1.1 Laws, 1.2 Regulators, 1.3 Administration and Enforcement Process**, as well as **5. Data Breach Reporting and Notification**.

4.3 Critical Infrastructure, Networks, Systems

Please see comments under **1.1 Laws, 1.2 Regulators, 1.3 Administration and Enforcement Process**, as well as **5. Data Breach Reporting and Notification**.

4.4 Denial of Service Attacks

Please see comments under **1.1 Laws, 1.2 Regulators, 1.3 Administration and Enforcement**

Process, as well as **5. Data Breach Reporting and Notification**.

4.5 Internet of Things (IoT), Software, Supply Chain, Other Data or Systems

Please see comments under **1.1 Laws, 1.2 Regulators, 1.3 Administration and Enforcement Process**, as well as **5. Data Breach Reporting and Notification**.

4.6 Ransomware

Please see comments under **1.1 Laws, 1.2 Regulators, 1.3 Administration and Enforcement Process** and **1.7 Key Developments**, as well as **5. Data Breach Reporting and Notification**.

5. Data Breach or Cybersecurity Event Reporting and Notification

5.1 Definition of Data Security Incident, Breach or Cybersecurity Event UK GDPR and DPA

Under the UK GDPR, “personal data breaches” are potentially reportable data security incidents. As explained in **1.3 Administration and Enforcement Process**, “personal data breach” is understood to mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Importantly, organisations' obligations to notify the ICO and affected data subjects do not arise in relation to every cybersecurity incident. Rather, the UK GDPR and DPA – and, in turn, applicable notification obligations – only apply where the breach involves personal data. As the Article 29 Working Party (WP29), the predecessor of the European Data Protection Board, notes in its guidance on personal data breaches: “all per-

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

sonal data breaches are security incidents, not all security incidents are necessarily personal data breaches”.

Further, the WP29 categorises personal data breaches in the following three breaches of security:

- confidentiality breach – unauthorised or accidental disclosure of, or access to, personal data;
- integrity breach – unauthorised or accidental alteration of personal data; and
- availability breach – where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Following the occurrence of a “personal data breach”, if the organisation is a controller then it needs to notify the ICO of the breach of the breach, unless the breach is “unlikely to result in a risk to the rights and freedoms of individuals”; such notice should be provided “without undue delay” and “where feasible, not later than 72 hours” after the controller became “aware” of the breach, having a “reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised”. If the organisation is a processor then it needs to notify the relevant controller “without undue delay” after it becomes “aware” of the breach.

In addition, controllers are required to notify affected data subjects “without undue delay” if the breach is “likely to result in a high risk to rights and freedoms” of such data subjects. Such data subjects’ notices are required to contain specific information, including the consequences of the breach and the steps that the controller has taken to address the breach. There are certain narrow exemptions from the obligation to notify

data subjects, such as where the compromised personal data was encrypted.

NIS Regulations

Under the NIS Regulations, different incident reporting obligations apply to OESs and RDSPs respectively. For OESs, cybersecurity event notification is required when any incident has a “significant impact” on the continuity of the essential service that the OES provides – determining this requires a fact-specific analysis of the number of users affected by the disruption of the service, the duration of the incident and the geographical area affected by the incident, as well as any other relevant guidance issued by their designated “competent authority”.

For RDSPs, notification is required where there will be a “substantial impact” on the provision of any relevant service. From 12 January 2022, the ICO, which is the lead regulator for RDSPs, must be notified by an RDSP where there is an incident which has a substantial impact on the provision of any digital services, including online marketplaces, online search engines and cloud computing services. It should be noted that, by comparison to the UK GDPR, notifiable incidents under the NIS Regulations need not always involve personal data – that is, cybersecurity incidents that do not involve personal data (such as, cyber-attacks on industrial control systems) could be notifiable under the NIS Regulations, but would not be notifiable under the UK GDPR if they do not involve personal data.

Comparable with the UK GDPR, both OESs and RDSPs must notify its relevant competent authority and the ICO respectively of an incident “without undue delay” and, in any event, no later than 72 hours after the OES or RDSP (as applicable) becomes aware of the incident.

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

PECR and CA 2003

Regulation 3 of PECR defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service. The security and breach notification requirements under Regulation 5 of PECR apply to personal data.

Under Regulation 5A of PECR, service providers are required to notify the ICO in the event of a personal data breach (as defined under Regulation 3 of PECR). Pursuant to Article 2(2) of the Notification Regulation, such notification must be made where feasible, no later than 24 hours after the detection of the personal data breach. A notification to the ICO is not required where an organisation is responsible for delivering part of the service, but does not have a direct contractual relationship with end users. In such cases, the organisation must notify the organisation that does have the contractual relationship with end users and that organisation must then notify the ICO. The service provider is also required to notify, without undue delay, the concerned subscriber or user where the breach is likely to adversely affect their personal data or privacy, unless the service provider can demonstrate to the ICO that the data was made unintelligible (eg, encrypted).

The security breach notification requirements under Section 105B of CA 2003 apply to public electronic communications networks and systems: network and service providers must notify Ofcom of security breaches which have a significant impact on the operation of a public electronic communications network. By contrast, CA 2003 does not define what is meant by a breach

of security. [Guidance on Security Requirements](#), published by Ofcom, provides further clarity on which incidents are likely to be significant and should therefore be reported.

Other Obligations

To the extent that organisations have contractually agreed with other organisations' or individuals' cybersecurity obligations that are broader or more rigorous than those set out in the specific cybersecurity law, the affected organisation would need to comply with those obligations. For example, many processors in the UK agree to notify controllers of "personal data breaches" within specific (short) timescales, rather than the more open-ended UK GDPR standard of "without undue delay". In such case, the processor would need to notify its controller within a specific (short) timescale. In addition, depending on the nature of the incident, and regardless of the specific cybersecurity law applicable to it, organisations in the UK may wish to notify appropriate UK law enforcement agencies, such as the National Crime Agency and Action Fraud.

5.2 Data Elements Covered

Please see comments under [5.1 Definition of Data Security Incident, Breach or Cybersecurity Event](#).

5.3 Systems Covered

Please see comments under [5.1 Definition of Data Security Incident, Breach or Cybersecurity Event](#).

5.4 Security Requirements for Medical Devices

In the UK, NHS Digital (the body responsible for information, data and IT systems in health and social care) has published a variety of guidance, including the [Data Security and Protection Toolkit](#) which is an online self-assessment

tool that all organisations must use if they have access to NHS patient data and systems. This includes an incident reporting tool which incorporates the notification requirements of the UK GDPR and the NIS Regulations. There is also a GDPR-focused [Respond to an NHS cyber alert](#) document which explains the intersection between medicine, personal data and cybersecurity.

At an EU level, but highly persuasive from a UK perspective, the Medical Device Coordination Group published updated guidance in June 2020 on cybersecurity for medical devices, which is intended to assist medical device manufacturers to meet the cybersecurity requirements in the Medical Devices Regulation and the In Vitro Diagnostic Regulation. According to the updated guidance, manufacturers must consider safety and cybersecurity throughout the lifecycle of a product – that is, they must integrate security “by design”. This concept closely aligns with the requirement of privacy by design under the UK GDPR. Manufacturers must also perform increased post-market surveillance and vigilance. Such post-market surveillance should address the following:

- operation of the device in the intended environment;
- sharing and dissemination of cybersecurity information and knowledge of cybersecurity vulnerabilities and threats across multiple sectors;
- vulnerability remediation; and
- incident response.

5.5 Security Requirements for Industrial Control Systems (and SCADA)

Please see comments under [5.1 Definition of Data Security Incident, Breach or Cybersecurity Event](#).

5.6 Security Requirements for IoT

It is expected that the security requirements under the PSTI will include, at least, the following requirements:

- all UK consumer connected products passwords be unique and incapable of being reset to any universal factory setting;
- manufacturers, importers and/or distributors of UK consumer connected products will have to provide a public point of contact for reporting vulnerabilities, and that these must be acted on in a timely manner; and
- manufacturers, importers and/or distributors of UK consumer connected products explicitly state the minimum length of time for which the device will receive security updates at the point of sale.

5.7 Requirements for Secure Software Development

Please see comments under [3.3 Legal Requirements and Specific Required Security Practices](#) and [5.1 Definition of Data Security Incident, Breach or Cybersecurity Event](#).

5.8 Reporting Triggers

Please see comments under [5.1 Definition of Data Security Incident, Breach or Cybersecurity Event](#).

5.9 “Risk of Harm” Thresholds or Standards

Please see comments under [5.1 Definition of Data Security Incident, Breach or Cybersecurity Event](#).

6. Ability to Monitor Networks for Cybersecurity

6.1 Cybersecurity Defensive Measures

While effective data security measures usually enhance individuals' privacy protections, excessive or intrusive cybersecurity measures can diminish individuals' privacy and freedoms. Therefore, to the extent that network monitoring or cybersecurity defensive measures involve the processing of personal data, the relevant UK GDPR obligations would need to be complied with. Key UK GDPR obligations would involve (among other things) providing UK GDPR-compliant notices to individuals, establishing a legal basis under the UK GDPR for such data processing – for example, relying on “legitimate interest”, and conducting a data protection impact assessment (DPIA) with respect to any data processing activities that are considered “high risk” under the UK GDPR.

Regarding the UK GDPR legal basis, while cybersecurity is acknowledged as a potential “legitimate interest”, the organisation would need to conduct a formal “legitimate interest assessment” to assess whether it has appropriately balanced as between its legitimate interest to implement network monitoring and other cybersecurity defensive measures while also protecting the individual's privacy interests.

In addition, certain kinds of employee monitoring measures (including those implemented for network monitoring and other cybersecurity defence reasons) are considered “high risk” under the UK GDPR. As a result, an organisation that intends to implement such measures would be required to conduct a DPIA prior to implementing such measures.

6.2 Intersection of Cybersecurity and Privacy or Data Protection

Please see comments under 6.1 Cybersecurity Defensive Measures.

7. Cyberthreat Information Sharing Arrangements

7.1 Required or Authorised Sharing of Cybersecurity Information

Please see comments under 5.1 Definition of Data Security Incident, Breach or Cybersecurity Event.

7.2 Voluntary Information Sharing Opportunities

A key information sharing organisation in the UK is the Cyber Security Information Sharing Partnership (CiSP). It is a joint industry and UK government initiative managed by the NCSC. The CiSP allows members to voluntarily exchange cyber-risk information in a secure environment, such that there are reductions to the impact of cyber-risks for UK businesses in general.

8. Significant Cybersecurity and Data Breach Regulatory Enforcement and Litigation

8.1 Regulatory Enforcement or Litigation GDPR and DPA

The key UK regulatory actions and litigation with respect to the British Airways, Marriott/Starwood and Interserve Group Ltd cybersecurity breaches have already been discussed in 1.6 System Characteristics and 1.7 Key Developments.

CMA

The ICO is taking cybersecurity increasingly seriously and this is demonstrated by the two

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

convictions it has helped secure in its prosecution of certain individuals. This has been for unauthorised access to personal data in both cases, and has led to the imprisonment of the defendants in question. The ICO explained that it is open to undertaking such prosecutions for data protection-related offences, using the CMA “to reflect the nature and extent of the offending and for the sentencing court to have a wider range of penalties available”.

8.2 Significant Audits, Investigations or Penalties

Please see comments under 1.6 System Characteristics, 1.7 Key Developments and 8.1 Regulatory Enforcement or Litigation.

8.3 Applicable Legal Standards

Please see comments under 1.1 Laws, 1.2 Regulators and 1.3 Administration and Enforcement Process.

8.4 Significant Private Litigation

Please see comments under 8.1 Regulatory Enforcement or Litigation. In addition, individuals are allowed to bring claims under the UK GDPR (including through representative actions). The British Airways group litigation and *Lloyd v Google* have already been noted. Under the CMA, individuals are able to bring a private prosecution without seeking permission from the DPP. The prosecution may be taken over by the CPS if the CPS determines that it is required. Private prosecutions have been brought by individuals (such as in connection with adversarial divorce proceedings). By contrast with the CMA, private prosecutions under the DPA require the consent of the DPP.

8.5 Class Actions

Please see comments under 8.4 Significant Private Litigation.

9. Cybersecurity Governance, Assessment and Resiliency

9.1 Corporate Governance Requirements

The matter is not relevant in this jurisdiction.

10. Due Diligence

10.1 Processes and Issues

The importance of conducting appropriate cybersecurity diligence in connection with corporate transactions is well illustrated by the ICO fining Marriot GBP18.4 million. More generally, M&A acquirers could (post-transaction) be directly liable for the M&A target’s UK GDPR and cybersecurity breaches if the acquirer were to, for example, exercise “decisive influence” over the target. Any regulatory fines could be levied as a percentage of the entire corporate group’s (including the acquirer’s) annual worldwide gross revenues. As a result, the target and acquirer are at risk for both regulatory fines (of up to 4% of annual worldwide group revenues) for non-compliance as well as private litigation brought by affected individuals and organisations.

In terms of corporate transaction-related cybersecurity diligence, an M&A acquirer will need to assess what diligence would be appropriate in the circumstances.

In many circumstances, a review of the target’s cybersecurity policies and procedures (including its written cybersecurity frameworks and certifications, incident response plans, and personal data breach register) would be itself appropriate. In some circumstances, more detailed cybersecurity diligence may be warranted, including forensic review and vulnerability of the target’s information technology and software systems,

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

as well as any products or platforms it offers to its customers.

After identifying any cybersecurity risks associated with the target, an M&A acquirer will then need to negotiate suitable representations and warranties with the target so as to address those risks appropriately. The M&A acquirer may also need to ensure that, post-transaction, the target undertakes measures to remedy any cybersecurity deficiencies that were not remedied previously.

10.2 Public Disclosure

The matter is not relevant in this jurisdiction.

11. Insurance and Other Cybersecurity Issues

11.1 Further Considerations Regarding Cybersecurity Regulation

The NCSC has issued guidance on cybersecurity insurance, which recommends the following:

- carrying out an audit of the current security measures an organisation has in place;

- getting certified under the Cyber Essentials and Cyber Essentials Plus schemes to get a discount on any insurance;
- ensuring there is a team of lawyers who can deal with contracts, technical experts who can manage IT systems and HR teams who can oversee cybersecurity processes and procedures;
- ensuring you understand your organisation so that an appropriate level and type of cover is set;
- checking if the cyber-insurance policy you are looking at covers claims for compensation by third parties in the event of a cyber-attack, or if personal data is lost as a result of a data breach at an organisation (for example, if a customer's personal data is lost); and
- checking the general limits of any policy chosen, including whether support will be provided both during and after a cybersecurity incident.

The UK government has also recognised that affordable and comprehensive cybersecurity insurance is a must with the Cyber Security Breaches Survey 2022 revealing that 39% of UK businesses have experienced a cyber-attack in the last 12 months, but only 19% of the UK businesses have an incident response plan.

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

Sidley Austin LLP is a premier global law firm with a practice highly attuned to the ever-changing international landscape. The firm advises clients around the globe, with more than 2,000 lawyers in 21 offices worldwide. Sidley maintains a commitment to providing quality legal services and to offering advice in litigation, transactional and regulatory matters spanning virtually every area of law. The firm's lawyers have wide-reaching legal backgrounds and are dedicated to teamwork, collaboration and superior client service. Sidley's lawyers help a

range of businesses address some of the most challenging matters concerning data protection, privacy, information security and incident response, data commercialisation, internet and computer law, intellectual property, information management and records retention, e-commerce, consumer protection and cybercrime. The firm advises clients with extensive operations in Europe, as well as in the USA, Asia and elsewhere, on developing and implementing global data protection programmes.

Authors



William Long is a partner of Sidley Austin. He is global co-leader of Sidley's highly ranked privacy and cybersecurity practice and leads the EU and UK data protection

practice. He advises international clients on a wide variety of GDPR, data protection, privacy, information security, social media, e-commerce and other regulatory matters. William has been a member of the European Advisory Board of the International Association of Privacy Professionals (IAPP) and on the DataGuidance panel of data protection lawyers. He is also on the editorial board of e-Health Law & Policy and assists with dplegal, which is a network for privacy professionals.



Eleanor Dodding is a managing associate at Sidley Austin. She provides practical and strategic advice to international clients regarding the EU and UK General Data Protection

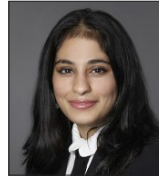
Regulation, e-privacy laws, international data transfers (including with respect to the Schrems II decision) and sector-specific privacy and cybersecurity laws. She also has experience in assisting clients with preparing for, and responding to, cybersecurity incidents.

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar,
Sidley Austin LLP



João Diogo Quartilho is an associate at Sidley Austin. He counsels international clients on a wide range of data protection, privacy and cybersecurity matters, including on

compliance with the GDPR, the ePrivacy Directive, international data transfers (including with respect to the Schrems II decision) and sector-specific privacy and cybersecurity laws. He also advises on privacy and cybersecurity issues in the context of due diligence of corporate transactions.



Subhalakshmi Kumar is an associate at Sidley Austin. She advises international clients on a wide range of data protection, privacy, and cybersecurity issues, including advising on

compliance with the EU General Data Protection Regulation (GDPR), the UK Data Protection Act and international data transfers. She has a particular interest in novel technologies including in relation to artificial intelligence and cyber-resilience.

Sidley Austin LLP

70 St Mary Axe
London
EC3A 8BE
UK

Tel: +44 20 7360 3600
Fax: +44 20 7626 7937
Email: wlong@sidley.com
Web: www.sidley.com

SIDLEY

Trends and Developments

Contributed by:

William Long, Eleanor Dodding, João Diogo Quartilho
and Subhalakshmi Kumar
Sidley Austin LLP see p.28

Introduction

The importance of cybersecurity for organisations continues to grow in 2023 and should remain a high-priority issue this year. In particular, the complexity and diversity of threat actors was exacerbated by a number of key factors, including Russia's invasion of Ukraine, which has made the UK one of the top three targeted countries in terms of cyber-attacks (the other two being the United States and Ukraine itself). 2022 also saw companies increase investment in their cybersecurity programmes, demonstrating a greater awareness of the importance of putting in place a strong and mature defence to system vulnerabilities. As a result of increased threats, the UK government continues to make strides in reforming its cybersecurity legislation, including notably through an expected update to the UK Network and Information Systems (NIS) Regulations.

Cybersecurity Threats in 2023: Ever More Complex and Diverse

There is growing appreciation that cyber-attacks are a threat to all types and sizes of business, with 39% of businesses confirming a cyber-attack in the latest [survey](#) by the UK government which covered the 12-month period from winter 2021 to winter 2022. The UK's National Cyber Security Centre (NCSC) also reported its [findings](#) for the period between September 2021 and August 2022. Firstly, the NCSC noted that despite geo-political factors such as in China and Russia driving concern around state sponsored attacks, financial gain remains a key motivator for threat actors. In this regard, ran-

somware attacks remain a key issue and the nature of such attacks is changing. Previously, ransomware attacks merely blocked systems through encryption, but now there is an increasing trend towards threat actors actually using data extortion as a core part of their business model. The ICO and NCSC also re-affirmed their calls for companies not to pay ransom demands and instead encouraged businesses to report – especially as evidence suggests that the payment of a ransom does not guarantee decryption of information or the return of exfiltrated data. The ICO also confirmed that payment will not reduce any penalties incurred through enforcement action.

Low sophistication cybercrime, including phishing, also continued to be a key issue, with 2.7 million cyber-related frauds in the 12 months to March 2022. Positively, the NCSC noted a greater awareness of these issues. One success has been its “Early Warning” initiative, a free service which is designed to inform an organisation of a potential cyber-attack as soon as possible – including proactively. The NCSC reported that, by August 2022, 34 million notifications to 7,500 members of its network had been sent.

Hacking of social media accounts to financially extort victims for access to their accounts or compromise their data, including by threatening to leak confidential information, has also grown over the past year. In 2021-22, there were a total of 8,023 reports of social media hacking to the NCSC, an increase of 23.5% on the previous year. The NCSC reported that “hackers for hire”

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

and “ransomware as a service” is increasingly present on the dark web and businesses will have to consider that attacks are now not just individuals or state forces, but those who operate at an organisational or business level.

There are also sectoral cybersecurity trends to track in 2023. For example, the public sector is now increasingly targeted with key bodies like the UK National Health Service (NHS) particularly vulnerable to attacks, along with key infrastructure bodies. Supply-chain attacks continue to be an issue of concern following the compromise of several major US and UK companies’ systems.

The NCSC also continues to issue practical guidance which should be monitored by all companies in 2023. Key points of note include the following.

- Relying on training and staff awareness is not enough, due to human error. Instead, organisations should utilise a multi-pronged approach, which includes technical and organisational safeguards against phishing.
- Regular testing and monitoring of a cybersecurity programme is essential and updates to technological safeguards through patching remain vital.
- Ensuring vendors have an appropriate cybersecurity programme in place. It should not be assumed that a vendor’s safeguards are sufficient.

Ukraine-Russia War Creates an Increasingly Global Cyber Threat

The most profound impact on the cybersecurity landscape in 2022 came from Russia’s invasion of Ukraine. War in Europe means a whole new form of cyberthreats, but it has also brought about convergence in security efforts between the UK and its allies and partners. The NCSC

identified four key threats that grew in the wake of the onset of war:

- cyber-enabled espionage;
- destructive cyber capabilities;
- cyber-enabled theft; and
- hacking and leaking data.

Various specific attacks were assessed and dealt with by the UK government before the physical invasion of Ukraine by Russian forces. For example, a month before the attack, Russian state actors deployed WhisperGate wiper malware against Ukrainian government offices. The NCSC also noted that information in relation to COVID-19 vaccine supply chains has been targeted, and that Russian groups have also developed a new form of malware known as “Sandworm”.

In addition, the energy crisis driven by the war in Ukraine has had significant cyber-implications. Cyber criminals have been targeting the extraction of financial credentials from consumers in emails ostensibly discussing rising energy costs.

It is clear that the Ukraine war continues to impact upon our cyber landscape and it is difficult for governments and commentators alike to predict what the long-term implications for cybersecurity will be. One positive impact has been increased collaboration and regulatory convergence between global allies in the cyber sphere: the NCSC regularly now works with their counterparts in the US (The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI)) and Australia (the Australian Cyber Security Centre (ACSC)) among others, to tackle cybercrime at a global level.

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

A number of key practical actions should be considered by businesses in relation to Russian threat actors:

- verify access controls – ensure passwords are unique, enable multi-factor authentication and remove old accounts as soon as possible;
- check your defences – update antivirus software, check firewall rules regularly and ensure configuration of common devices or work devices are secure;
- have a response plan – know how you will respond to an incident through an incident response plan, breach log and table-top exercises.

Cybersecurity Reform

The UK government continues to develop its package of reforms as part of its first [Cyber Security Strategy for 2022–30](#). In particular, there is now a legislative framework on the internet of things (IoT) with the new Product Security and Telecommunications Infrastructure Act (PSTI) receiving royal assent on 6 December 2022. The PSTI allows the Secretary of State for Digital Culture Media and Sport (DCMS) to introduce regulations which will impose security requirements on both manufacturers and users of “relevant connectable products”, impacting all internet connected and network connected products.

New legislation is also in the works in sectors where the UK government perceives there to be the greatest potential impact of cyber-attacks, such as to critical service providers. For example, on 30 November 2022, the UK government [confirmed](#) its plans to strengthen the Network and Information Systems (NIS) Regulations (Regulations), which will impact energy companies, the NHS, and important digital services like cloud computing providers and online search engines.

Importantly, this version of NIS also expands on the previous regulations which were in place. NIS now applies to entities such as outsourced IT providers and “managed service providers” of digital services – meaning that many more technology companies will be brought within scope of the stringent cybersecurity obligations under NIS. It is expected that the Regulations will require essential and digital service providers to improve cyber-incident reporting and also to notify in a wider range of circumstances than is currently required, including when no disruption has been faced. The Regulations will also implement a cost recovery system to reduce the burden on UK taxpayers when large scale incidents occur.

In addition, the UK government has published a consultation entitled [Data: a new direction](#). In June 2022, the UK government released its [response](#) to the consultation, having heard from key stakeholders, including the ICO, on its proposed reforms. Of note is that the UK government has now abandoned its plan to change personal data breach reporting requirements. The original consultation proposals had suggested that organisations may in the future be able to avoid reporting a breach where an incident is considered to be “not material”. This was a change from the previous test for reporting a breach under the GDPR, which was that an organisation had to report to the ICO unless the incident was “unlikely” to result in a risk to people’s rights and freedoms. The UK government recognised in its response that their plans lacked detail in terms of when a non-material risk would not need to be reported, and instead committed to investing in producing further guidance on breach reporting. It will be interesting to see the new guidance and how this will interplay with other cyber-related guidance. It will be important in 2023 to monitor any new data protection leg-

UK TRENDS AND DEVELOPMENTS

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar,
Sidley Austin LLP

isolation arising out of the consultation and how any cybersecurity issues are addressed.

This article has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and the receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers. The content therein does not reflect the views of the firm.

UK TRENDS AND DEVELOPMENTS

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar, Sidley Austin LLP

Sidley Austin LLP is a premier global law firm with a practice highly attuned to the ever-changing international landscape. The firm advises clients around the globe, with more than 2,000 lawyers in 21 offices worldwide. Sidley maintains a commitment to providing quality legal services and to offering advice in litigation, transactional and regulatory matters spanning virtually every area of law. The firm's lawyers have wide-reaching legal backgrounds and are dedicated to teamwork, collaboration and superior client service. Sidley's lawyers help a

range of businesses address some of the most challenging matters concerning data protection, privacy, information security and incident response, data commercialisation, internet and computer law, intellectual property, information management and records retention, e-commerce, consumer protection and cybercrime. The firm advises clients with extensive operations in Europe, as well as in the USA, Asia and elsewhere, on developing and implementing global data protection programmes.

Authors



William Long is a partner of Sidley Austin. He is global co-leader of Sidley's highly ranked privacy and cybersecurity practice and leads the EU and UK data protection

practice. He advises international clients on a wide variety of GDPR, data protection, privacy, information security, social media, e-commerce and other regulatory matters. William has been a member of the European Advisory Board of the International Association of Privacy Professionals (IAPP) and on the DataGuidance panel of data protection lawyers. He is also on the editorial board of e-Health Law & Policy and assists with dplegal, which is a network for privacy professionals.



Eleanor Dodding is a managing associate at Sidley Austin. She provides practical and strategic advice to international clients regarding the EU and UK General Data Protection

Regulation, e-privacy laws, international data transfers (including with respect to the Schrems II decision) and sector-specific privacy and cybersecurity laws. She also has experience in assisting clients with preparing for, and responding to, cybersecurity incidents.

UK TRENDS AND DEVELOPMENTS

Contributed by: William Long, Eleanor Dodding, João Diogo Quartilho and Subhalakshmi Kumar,
Sidley Austin LLP



João Diogo Quartilho is an associate at Sidley Austin. He counsels international clients on a wide range of data protection, privacy and cybersecurity matters, including on

compliance with the GDPR, the ePrivacy Directive, international data transfers (including with respect to the Schrems II decision) and sector-specific privacy and cybersecurity laws. He also advises on privacy and cybersecurity issues in the context of due diligence of corporate transactions.



Subhalakshmi Kumar is an associate at Sidley Austin. She advises international clients on a wide range of data protection, privacy, and cybersecurity issues, including advising on

compliance with the EU General Data Protection Regulation (GDPR), the UK Data Protection Act and international data transfers. She has a particular interest in novel technologies including in relation to artificial intelligence and cyber-resilience.

Sidley Austin LLP

70 St Mary Axe
London
EC3A 8BE
UK

Tel: +44 20 7360 3600
Fax: +44 20 7626 7937
Email: wlong@sidley.com
Web: www.sidley.com

SIDLEY

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com