Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2025

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

UK: Law and Practice & Trends and Developments

William Long, Francesca Blythe, Eleanor Dodding and Anila Rayani
Sidley Austin LLP

UK

Law and Practice

Contributed by:
William Long, Francesca Blythe, Eleanor Dodding and Anila Rayani
Sidley Austin LLP

Contents

1. General Overview of Laws and Regulators p.5
1.1 Cybersecurity Regulation Strategy p.5
1.2 Cybersecurity Laws p.5
1.3 Cybersecurity Regulators p.7

2. Critical Infrastructure Cybersecurity p.8
2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.8
2.2 Critical Infrastructure Cybersecurity Requirements p.9
2.3 Incident Response and Notification Obligations p.9
2.4 State Responsibilities and Obligations p.10

3. Financial Sector Operational Resilience Regulation p.10
3.1 Scope of Financial Sector Operational Resilience Regulation p.10
3.2 ICT Service Provider Contractual Requirements p.11
3.3 Key Operational Resilience Obligations p.11
3.4 Operational Resilience Enforcement p.12
3.5 International Data Transfers p.12
3.6 Threat-Led Penetration Testing p.13

4. Cyber-Resilience p.13
4.1 Cyber-Resilience Legislation p.13
4.2 Key Obligations Under Legislation p.13

5. Security Certification for ICT Products, Services and Processes p.16
5.1 Key Cybersecurity Certification Legislation p.16

6. Cybersecurity in Other Regulations p.16
6.1 Cybersecurity and Data Protection p.16
6.2 Cybersecurity and AI p.18
6.3 Cybersecurity in the Healthcare Sector p.18

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 and has more than 2,300 lawyers in 21 offices worldwide. Sidley Austin maintains a commitment to providing quality legal services and offering advice on 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. The team helps 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, IP, information management and records retention, e-commerce, consumer protection, and cybercrime. Sidley Austin 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 at Sidley Austin LLP, where he leads the EU and UK data protection practice and is global co-leader of the firm's highly ranked privacy and cybersecurity practice. William advises international clients on a wide variety of AI, cyber, and digital data laws, as well as data protection, privacy, information security, social media, e-commerce and other regulatory matters. He has been a member of the International Association of Privacy Professionals (IAPP)'s European Advisory Board and on the DataGuidance panel of data protection lawyers. William has also been on the editorial board of "e-Health Law & Policy" and assists with dplegal, a network for privacy professionals.

Francesca Blythe is a partner at Sidley Austin LLP and advises international clients on a wide range of privacy, cybersecurity, and emerging technology issues, including on privacy and cybersecurity compliance strategies. She has also counselled clients in preparing for, and responding to, data breaches of varying sizes. Francesca co-leads Sidley Austin's benchmarking group for in-house data privacy professionals (dplegal) in the life sciences sector and was previously in-house counsel at the largest international health and beauty retailer in Asia and Europe. While there, she regularly gave advice on compliance and strategies relating to data protection laws and assisted in the planning and delivery of a global privacy compliance project.

Eleanor Dodding is a senior managing associate at Sidley Austin LLP. 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 regard to the Schrems II decision), and sector-specific privacy and cybersecurity laws. Eleanor also has experience in assisting clients with preparing for, and responding to, cybersecurity incidents.

Anila Rayani is an associate at Sidley Austin LLP. She advises international clients on various data protection, privacy, and cybersecurity matters, including the EU and UK General Data Protection Regulation, e-privacy laws, and emerging AI and cyber frameworks. Anila also has experience investigating and responding to complex cross-border cybersecurity incidents and personal data breaches, as well as dealing with regulatory inquiries.

Sidley Austin LLP

70 St Mary Axe
London
EC3A 8BE
UK

Tel: +44 020 7360 3600
Fax: +44 020 7626 7937
Web: www.sidley.com

SIDLEY

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

The UK cybersecurity legal system is well developed and is similar to the legal systems across the European Economic Area (EEA), rather than the USA – although post-Brexit, divergence in approach to cybersecurity regulation by the EU and the UK are starting to emerge. Since the GDPR came into force in 2018, the enforcement of cybersecurity rules in the UK continues to be a focus, particularly by the UK data protection regulator, the Information Commissioner's Office (ICO). In 2025, the UK looks set to introduce new legislation to address the changing cyberthreat landscape and more closely align UK law with developments in the EU (such as the Network and Information Systems Directive 2 (the "NIS 2 Directive") – see **2. Critical Infrastructure Cybersecurity** for further detail.

The UK government has also signalled an overhaul of its ability to assist and promote cybersecurity through its national cyber strategy for 2022 (the "National Cyber Strategy"), as well as through its government-specific Government Cyber Security Strategy for 2022–30. The National Cyber Strategy takes a "whole of society" approach, with the aim of shifting the burden of cybersecurity from individual citizens to the organisations and professionals best placed to manage cyber-risks. The National Cyber Strategy is comprised of five pillars, which it is working to achieve by 2025:

- strengthening the UK cyber ecosystem – by investing in people and skills, and deepening the partnership between government, academia and industry;
- building a resilient and prosperous digital UK – by reducing cyber-risks so that businesses can maximise the economic benefits of digital technology and provide more security for UK citizens online;
- taking the lead in technologies vital to cyber power – by building industrial capacity and developing frameworks to secure future technologies;
- advancing UK global leadership and influence for a more secure, prosperous and open international order – by working with government and industry partners and sharing the expertise that underpins UK cyber power; and
- detecting, disrupting and deterring adversaries to enhance UK security in and through cyberspace – by making more integrated, creative and routine use of the UK's full spectrum of levers.

The National Cyber Strategy also proposes a number of regulatory reforms, including but not limited to increasing the scope of the Network and Information Systems Regulations (the "NIS Regulations") (see **2. Critical Infrastructure Cybersecurity** for further detail).

1.2 Cybersecurity 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 that are established outside the UK but are processing personal data of individuals located in the UK, are derived from the UK General Data Protection Regulation (the "UK GDPR"), as supplemented by the UK Data Protection Act 2018 (DPA).

The UK GDPR applies to the security of "personal data" (ie, 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 **6.1 Cybersecurity and Data Protection**). 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, the NIS Regulations currently 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 report certain cybersecurity incidents that affect such organisations. On 17 July 2024, the UK government announced the Cybersecurity and Resilience Bill (the "CS&R Bill"), which would expand the remit of the NIS Regulations to protect more digital services and supply chains. Please see **2.1 Scope of Critical Infrastructure Cybersecurity Regulation** for additional information on the proposed updates to the NIS Regulations via the CS&R Bill.

Thirdly, the Product Security and Telecommunications Infrastructure Act 2022 (the "PSTI Act"), which came into force on 29 April 2024, requires manufacturers, importers and distributors of UK consumer-connected products to meet certain cybersecurity standards. This includes more stringent security requirements (eg, default password requirements and minimum support periods for providing security updates) and requirements to investigate any compliance failures and take remediation action, as well as notify relevant authorities and other third parties about such compliance failures (see **4.2 Key Obligations Under Legislation**).

Fourthly, the Computer Misuse Act 1990 (CMA) is the UK's primary legislation with regard 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 computer – ie, 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 (the "PECR"), the EU Notification Regulations 611/2013 (the "Notification Regulation"), and the Communications Act 2003 (the "CA 2003") 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, Financial Conduct Authority (FCA) rules (applicable to FCA-regulated firms), the Payment Services Regulations 2017 (PSRs) (which transposed the Second EU Payment Services Directive into English law and apply to payment service providers), and the Official Secrets Act 1989 (OSA) (which is 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 ICO and sector-specific regulators such as the 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, the Office of Communications (Ofcom) and the FCA to form the Digital Regulation Co-operation 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, the PSRs, the OSA, the IPA, the RIPA and other sector-specific or specialised laws or the common-law duty of confidence are not further considered in this guide.

1.3 Cybersecurity 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 of 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. Please note that prosecutions under the DPA can only be brought by the ICO or by (or with the consent of) the Director of Public Prosecutions (DPP).

NIS Regulations

With regard to the NIS Regulations, the "competent authority" is determined on an industry-by-industry basis through the Department for Science Innovation and Technology (DSIT), which oversees the implementation of the NIS Regulations across the UK. For OESs in the oil sector, for example, the competent authority in England, Scotland and Wales is the Secretary of State for Business, Energy and Industrial Strategy – whereas 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 Cybersecurity Security Centre (NCSC), which offers 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

As regards the PECR, the ICO may audit the compliance of service providers pursuant to Regulation 5A of the PECR. Notifiable personal data breaches under Regulation 5A of the PECR

must be reported to the ICO. The ICO is, in turn, responsible for investigating the breach and taking any subsequent enforcement action.

However, with regard to the CA 2003 (which is a companion legislation to the 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.

CMA

Although 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), which is 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. See **4.2 Key Obligations Under Legislation** for more information.

PSTI

The Office for Product Safety and Standards is responsible for enforcing the PSTI Act. Non-compliance with the PSTI Act can result in fines of up to GBP10 million or 4% of a company's global turnover (whichever is greater), as well as up to GBP20,000 per day in the case of an ongoing contravention.

National Cybersecurity Security Centre

The NCSC is the key UK cybersecurity agency, co-ordinating UK cybersecurity policy and technical standards, particularly with regard 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 in order to allow for improved cybersecurity across Europe.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

The regulation of cybersecurity for critical infrastructure in the UK is primarily governed by the NIS Regulations. See **1.2 Cybersecurity Laws** for a summary of the scope of the NIS Regulations.

On 17 July 2024, the UK government introduced the CS&R Bill, intended to strengthen UK defences against cyber-attacks and protect critical infrastructure. The briefing note on the CS&R Bill suggests it will update the UK's cyber regulatory framework by:

- expanding the scope of the NIS Regulations to cover "more digital services and supply chains";
- giving further power to regulators to ensure measures are being implemented; and
- mandating increased incident reporting to provide a better picture of the threat landscape and cyber-attacks.

It is expected that the CS&R Bill will be introduced in Parliament in 2025.

2.2 Critical Infrastructure Cybersecurity Requirements

OESs and RDSPs are required under the NIS Regulations to implement appropriate and proportionate technical and organisational measures to ensure a level of security appropriate to the risk posed.

RDSPs

For RDSPs, these requirements are supplemented by the Commission Implementing Regulation (EU) 2018/151 (the "DSP Regulation"). In summary, RDSPs must take account of the following.

- The security of systems and facilities – measures in this area should cover systematic management of network and information systems, physical and environmental security measures, security of supplies and access controls to systems.
- Incident handling – measures should include incident detection processes and procedures, processes and policies on incident reporting, incident response and incident assessment. See **2.3 Incident Response and Notification Obligations** for further detail.
- Business continuity management – this is the capability to maintain or restore the delivery of services to acceptable predefined levels following a disruptive incident.
- Monitoring, auditing and testing – measures should establish and maintain policies and processes concerning the assessment, inspection and verification of systems.
- Compliance with international standards – measures are not specified by the DSP Regulation but, instead, the NIS Regulations refer to "standards" as:
  (a) standards adopted by an international standardisation body as specified in Regulation 1025/2012; and/or
  (b) any European, national, or internationally-accepted standards and specifications relevant to the security of networks and information systems.

The ICO notes that examples of appropriate standards may include ISO/IEC 27001 on information security management systems and ISO/IEC 22301 on business continuity management systems, as well as any other related standards.

OESs

OESs are subject to similar requirements as RDSPs in that they must also take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies, and subject to guidance from the relevant competent authority (which, as noted in **1.3 Cybersecurity Regulations** (NIS Regulations), is on a sector-specific basis).

2.3 Incident Response and Notification Obligations

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. As from 12 January 2022, the ICO (which is the lead regulator for RDSPs) must be notified by an RDSP where there is an incident that 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, in comparison with 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.

Under the NIS Regulations, as with the UK GDPR, OESs and RDSPs must notify their 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.

The NIS Regulations require that OESs and RDSPs adopt "appropriate and proportionate" technical and organisational security measures, as well as "appropriate" measures to prevent and minimise the impact of incidents affecting those systems (taking into account the state of the art), so as to ensure the continuity of the essential services that the OES provides. Although 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.

2.4 State Responsibilities and Obligations

This not applicable in the UK.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

In the UK, operational resilience in the financial sector is primarily addressed by the FCA, the Prudential Regulatory Authority (PRA) and the Bank of England in their rules and guidance on requirements to strengthen operational resilience in the financial services sector – for example, the FCA's rules on operational resilience under Chapter 15A of its Senior Management Arrangements, Systems and Controls Sourcebook and the PRA's supervisory statement "Operational resilience: Impact tolerances for important business services" (SS1/21) (collectively, the "Operational Resilience Requirements"), which were published on 31 March 2022 and address how firms identify, map, test and enhance their important business services to withstand disruptions. The requirements for UK firms to have performed mapping and testing so that they are able to remain within impact tolerances for each important business service are required to be in place by no later than 31 March 2025. The rules are intended to align closely (albeit not entirely) with international standards and other regimes, such as the EU's Digital and Operational Resilience Act (DORA).

In November 2024, the FCA and the PRA published a joint policy statement, "Operational resilience: Critical third parties to the UK financial sector" (PS16/24) (the "CTP Policy Statement"). This confirmed that operational resilience remains a priority for the regulators and focuses, among other things, on further defining obligations with resgard to critical third parties (CTPs) (see **3.2 ICT Service Provider Contractual Requirements** for further detail).

3.2 ICT Service Provider Contractual Requirements

As noted in **3.1 Scope of Financial Sector Operation Resilience Regulation**, CTPs are a key focus of UK financial services operational resilience. The CTP Policy Statement introduces new rules that will apply to a CTP designated under the regime.

Under the applicable rules, CTPs will need to:

- meet the minimum resilience standards in respect of any material services that they are providing to financial services firms;
- comply with six "fundamental rules" that will apply to all the services a CTP provides, including having effective risk strategies and dealing with the FCA or PRA (as applicable) in a co-operative manner; and
- comply with eight "operational risk and resilience requirements" that will apply to a CTP's material services, such as the requirement to appropriately manage incidents that may adversely affect (or may reasonably be expected to adversely affect) the delivery of a material service.

The new regime for CTPs was created under the Financial Services and Markets Act 2023, which amended the Financial Services and Markets Act 2000 (FSMA). The relevant provisions allow the UK Treasury to designate a person who provides services to regulated firms and financial market infrastructures as "critical". CTPs will typically be service providers that provide certain outsourced and third-party services to large numbers of financial institutions and whose services are very difficult to substitute. Although the concepts in FSMA are broadly analogous to DORA, the criteria for designation and the scope of regulatory powers differ in several important respects.

3.3 Key Operational Resilience Obligations

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's 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 anything relating to the firm of which that regulator would reasonably expect notice".

In relation to Principle 11, the FCA has confirmed that regulated firms 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 PRA 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 personal 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 Cyber Security Information Sharing Partnership (CiSP) platform. The CiSP is a key information-sharing organisation in the UK. 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.

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. By way of example, payment services providers are required to report major operational and security incidents pursuant to the PSRs.

For CTPs, the rules established by CTP Policy Statement introduce a phased approach to notifications in relation to incidents affecting CTP services, such as those that impact the availability, authenticity, integrity, or confidentiality of assets. This reporting will consist of:

- an initial notification, without undue delay, to the relevant parties after the CTP is aware that the relevant incident has occurred;
- one or more intermediate incident reports as needed; and
- a final incident report.

Looking forward, the Operational Resilience Requirements will require financial services firms to comply with a number of obligations around operational resilience, including:

- performing mapping and scenario testing (including for cyber-related disruptions);
- investing to enable a firm to operate within its impact tolerances and respond effectively and recover quickly when disruption does occur;
- documenting and maintaining operational resilience policies and procedures;
- assigning clear roles and responsibilities within the firm; and
- engaging with key stakeholders (eg, regulators, clients, suppliers, and CTPs).

On 13 December 2024, the PRA and FCA published further consultation papers – respectively, "Operational resilience: Operational incident and outsourcing and third-party reporting" (PRA CP17/24) and "Operational Incident and Third-Party Reporting" (FCA CP24/28). These propose a framework for reporting operational incidents and notification and reporting of material third-party arrangements. Under the proposals, the PRA and FCA will expect firms to report incidents meeting certain thresholds. The consultation papers are open for comments until 13 March 2025.

3.4 Operational Resilience Enforcement

The FCA and PRA have a broad legislative mandate and powers to enforce rules made under the CTP regime against designated CTPs. As this is a new regime, it remains to be seen how such powers will be exercised.

3.5 International Data Transfers

This is not applicable in the UK.

3.6 Threat-Led Penetration Testing

See **3.3 Key Operational Resilience Requirements** for the upcoming Operational Resilience Requirements, which will include testing requirements.

In addition, the CBEST programme is a cyber-assessment tool to assist UK firms with assessing the cyber-resilience of key financial institutions through security testing performed in "live" corporate environments. On 13 December 2024, the FCA (together with the Bank of England and the PRA) published their annual CBEST thematic report (the "CBEST Report"). The CBEST Report contains cyber-resilience good practice recommendations and insight, including from the NCSC, for firms to help them maintain their operational resilience. The good practice recommendations are the result of a programme that assesses the cyber-resilience of systemic financial institutions through live testing. The report highlights the importance of building a strong foundation of cyberhygiene to prevent common cyber-incidents, including training and awareness and robust authentication.

The key areas of focus based on the 2024 CBEST Report are:

- cybersecurity risks to assets and individuals;
- cyber-risk management and impact-based approaches to the protection of key resources (people, process, technology and data);
- detection and response capabilities leveraging the latest threat intelligence; and
- cyber-incident response to eradicate threats and mitigate impacts.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

As outlined in **1.2 Cybersecurity Laws**, there are a number of laws that supplement the UK's cyber-resilience strategy alongside the NIS Regulations. Please refer to **4.2 Key Obligations Under Legislation** for more information.

4.2 Key Obligations Under Legislation

PSTI Act

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 cybersecurity risk for connected products made available in the UK. Similar obligations also apply to importers and distributors. These include:

- duty to comply with security requirements as defined by the Secretary of State;
- duty to investigate and take action in relation to compliance failures – this 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 of investigations and compliance failures 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 PSTI Act provides for the power of the Secretary of State to deem compliance with security requirements. This is further elaborated in the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 (the

"PSTI Regulations"), which set out conditions for deemed compliance with security standards, including compliance with relevant parts of ETSI EN 303 645 or – in some cases – ISO/IEC 29147.

Schedule 1 of the PSTI Regulations includes the following security requirements for manufacturers:

- all UK consumer connected products passwords must be unique and incapable of being reset to any universal factory setting;
- manufacturers, importers and/or distributors of UK consumer-connected products must provide a public point of contact for reporting vulnerabilities and 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.

CMA

As mentioned in **1.2 Cybersecurity Laws**, a key offence under the CMA (Section 1) is where a defendant obtains "unauthorised access" to a computer. Although 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. By way of 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 that has facilitated the offending may have passed through a server based in a relevant country of the UK.

An offence committed under the CMA is prosecuted through the UK courts by the CPS. When 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. Offences under the CMA can carry 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.

The UK government continues to progress amendments to the CMA, as for many years commentators have stated that the CMA has failed to keep pace with the cybersecurity landscape. Commentators highlight issues with the ambiguity around the meaning of "authorisation" and its subsequent impact on cybersecurity professionals, as well as issues with the current jurisdictional scope of the CMA, given the international nature of many cybersecurity incidents. In November 2023, the UK government published responses to a consultation on proposed CMA reforms, noting that work will continue on engagement with private and public sector organisations to understand further impacts and mitigations in this area before it is considered for legislation.

PECR and CA 2003

Regulation 5(1A) of the 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 regard 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 the PECR.

Guidance on Security Requirements published by Ofcom in relation to the CA 2003 states that it is necessary to establish "clear lines of accountability, 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 that exceed those in the Cyber Essentials scheme; and
- the importance of intelligence-led vulnerability testing to manage cyber-risks.

Regulation 2(1) of the PECR defines a "personal data breach" as a breach of security leading to the accidental or unlawful destruction, loss, alteration, or 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 the PECR apply to personal data.

Under Regulation 5A of the PECR, service providers are required to notify the ICO in the event of a personal data breach (as defined under Regulation 3 of the 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 105K(1)(a) of the CA 2003 apply to public electronic communications networks and systems: network and service providers must notify Ofcom of security breaches that have a significant impact on the operation of a public electronic communications network. Section 105(A) of the CA 2003 broadly defines a "security compromise" as including "anything that compromises the availability, performance or functionality of the network or service". In

determining whether the effect that a security compromise has – or would have – on the operation of a network or service is "significant", certain matters should be considered, including the length of the period during which the operation of the network or service is or would be affected, the number of affected persons, the geographical size and location affected, and the extent to which activities of persons who use the network or service are or would be affected by the effect on the operation of the network or service.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

There are numerous cybersecurity frameworks that are expressly or implicitly recognised by UK cybersecurity regulators. By way of 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.

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

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

As mentioned in **1.2 Cybersecurity Laws**, the UK GDPR and the DPA contain cybersecurity obligations in relation to the processing of personal data. 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 them goods or services or to monitor their behaviour.

The UK GDPR requires that controllers and processors implement "appropriate" technical and organisational security measures, taking into account the state of the art, costs of implementation, and the nature, scope, context and purposes of the processing of personal data, as well as the 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, which are:

- 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 and 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 which 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), as well as 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.

The UK GDPR and the DPA continue to be enforced by the ICO, including with regard to cybersecurity matters, but only to the extent that 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 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. Although 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 in order 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.

6.2 Cybersecurity and AI

On 26 November 2023, the US Cybersecurity and Infrastructure Security Agency (CISA), together with the UK's NCSC, published joint Guidelines for Secure AI System Development (the "AI Guidelines"). The AI Guidelines aim to ensure that developers take a "secure by design" approach, integrating cybersecurity into the development process from the outset and throughout. The AI Guidelines cover secure design, secure development, secure deployment, and secure operation and maintenance. Relatedly, in its annual review published on 3 December 2024, the NCSC noted the significant advances in AI that will enable and enhance existing challenges associated with cybersecurity.

Work is currently underway by the DSIT to produce a sector agnostic Code of Practice on Cyber Security of AI (the "AI COP") to establish the minimum cybersecurity standards that developers and system operators should incorporate when building and using AI solutions. The AI COP, which is voluntary, is based on the AI Guidelines and is intended to sit alongside the UK government's 2023 White Paper "A pro-innovation approach to AI regulation", which includes "Safety, Security and Robustness" as one of the five key principles – the focus of the AI COP. The AI COP is structured around 12 principles and stakeholders to which each principle primarily applies are identified. Requirements include AI security awareness training, system design and dataset considerations, incorporating threat-modelling into the risk management process, and evaluation and testing. The consultation on the AI COP closed on 9 August 2024 and the UK government's response is anticipated – although no timeline has been set.

6.3 Cybersecurity in the Healthcare Sector

Under the NIS Regulations, NHS trusts, foundation trusts, integrated care boards, and certain other healthcare providers are designated as OESs. Consequently, these healthcare providers are required to comply with the obligations of an OES as described in **2.2 Critical Infrastructure Cybersecurity Requirements**.

Medical devices in scope of the Medical Devices Regulations 2002 are expressly excluded from the PSTI Act. However, the UK government is expected to continue its overhaul of the UK's medical devices legislative framework following the application of the Medicines and Medical Devices Act 2021 (the "MMD Act"). The MMD Act includes powers for the Secretary of State to introduce regulations in relation to the manufacture of medical devices. In February 2024, the Department for Health and Social Care (DHSC) confirmed that it would be introducing a package of legislative reform for UK medical devices. In December 2024, the Medicines & Healthcare products Regulatory Agency (MHRA) issued a

revised roadmap for reform (the "Roadmap"), which stated that new guidance will be published on cybersecurity requirements for software included as part of a medical device.

The MHRA has produced a number of work packages in their proposed Software and AI as a Medical Device Change Programme, with Work Package WP5 dedicated to "Cyber Secure Medical Devices". This work package focuses on ensuring that cybersecurity is adequately reflected in software as a medical device (SaMD) requirements and explains that secondary legislation will be developed to impose cybersecurity and IT requirements to guard against cybersecurity risks in medical devices and in vitro diagnostics (IVDs) that may result in device malfunction, loss or tampering with personal data, damage to the device, and ultimately injury to the patient. Guidance will be developed on cybersecurity issues in the life cycle management processes of medical devices and IVDs and on the reporting of cybersecurity vulnerabilities.

NHS Digital (the body responsible for information, data and IT systems in health and social care in the UK) 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 that incorporates the notification requirements of the UK GDPR and the NIS Regulations. There is also a GDPR-focused document entitled "Respond to an NHS Cyber-Alert", which explains the intersection between medicine, personal data, and cybersecurity.

At an EU level (albeit highly persuasive, rather than legally binding, from a UK perspective), the Medical Device Co-Ordination Group published updated guidance in June 2020 on cybersecurity for medical devices, which is intended to assist medical device manufacturers in meeting the cybersecurity requirements in the EU's Medical Devices Regulation and the In Vitro Diagnostic Regulation. According to the updated guidance, manufacturers must consider safety and cybersecurity throughout the life cycle 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.

The MHRA clearly stated in its Roadmap the regulations will move the UK towards greater alignment of the cybersecurity requirements for medical devices with the approach taken by the EU and other international regulators.

Lastly, it is worth mentioning that – rather than taking a separate approach to any AI-enabled product – the UK's approach to regulating cybersecurity risks resulting from AI is sector-specific. In the healthcare space, the MHRA has announced in its Policy Paper "Impact of AI on the regulation of medical products" of April 2024 that it will follow a principles-based approach in order to avoid constraining innovation, including the guidance on cybersecurity for AI as expected to be published in spring 2025.

Trends and Developments

Contributed by:
William Long, Francesca Blythe, Eleanor Dodding and Anila Rayani
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 and has more than 2,300 lawyers in 21 offices worldwide. Sidley Austin maintains a commitment to providing quality legal services and offering advice on 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. The team helps 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, IP, information management and records retention, e-commerce, consumer protection, and cybercrime. Sidley Austin 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 at Sidley Austin LLP, where he leads the EU and UK data protection practice and is global co-leader of the firm's highly ranked privacy and cybersecurity practice. William advises international clients on a wide variety of AI, cyber, and digital data laws, as well as data protection, privacy, information security, social media, e-commerce and other regulatory matters. He has been a member of the International Association of Privacy Professionals (IAPP)'s European Advisory Board and on the DataGuidance panel of data protection lawyers. William has also been on the editorial board of "e-Health Law & Policy" and assists with dplegal, a network for privacy professionals.

Francesca Blythe is a partner at Sidley Austin LLP and advises international clients on a wide range of privacy, cybersecurity, and emerging technology issues, including on privacy and cybersecurity compliance strategies. She has also counselled clients in preparing for, and responding to, data breaches of varying sizes. Francesca co-leads Sidley Austin's benchmarking group for in-house data privacy professionals (dplegal) in the life sciences sector and was previously in-house counsel at the largest international health and beauty retailer in Asia and Europe. While there, she regularly gave advice on compliance and strategies relating to data protection laws and assisted in the planning and delivery of a global privacy compliance project.

Contributed by: William Long, Francesca Blythe, Eleanor Dodding and Anila Rayani, **Sidley Austin LLP**

Eleanor Dodding is a senior managing associate at Sidley Austin LLP. 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 regard to the Schrems II decision), and sector-specific privacy and cybersecurity laws. Eleanor also has experience in assisting clients with preparing for, and responding to, cybersecurity incidents.

Anila Rayani is an associate at Sidley Austin LLP. She advises international clients on various data protection, privacy, and cybersecurity matters, including the EU and UK General Data Protection Regulation, e-privacy laws, and emerging AI and cyber frameworks. Anila also has experience investigating and responding to complex cross-border cybersecurity incidents and personal data breaches, as well as dealing with regulatory inquiries.

Sidley Austin LLP

70 St Mary Axe
City of London
London
EC3A 8BE
UK

Tel: +44 020 7360 3600
Fax: +44 020 7626 7937
Web: www.sidley.com

SIDLEY

Cyber-Resilience in the UK: An Overview

Cyber-resilience is a sector-agnostic issue that is continuing to grow in importance; a cybersecurity breach can have a significant financial impact on an organisation and cause untold damage to brand and reputation. As the world grows ever more dependent on technology such as AI, cybersecurity awareness and good cyber-hygiene become increasingly fundamental to the UK's overall resilience. Consequently, cybersecurity has been a UK government priority.

Despite a change in government in 2024, the pace of cybersecurity reform remained consistent – with the passing and proposing of a number of new laws, as well as the publication of several consultations on draft guidance. Supply chain cybersecurity resilience was a key theme and is expected to continue in 2025, likely influenced by the plethora of new EU cybersecurity laws (such as the Network and Information Security Directive 2 ("NIS2")). Consequently, it is expected that cybersecurity legislation will remain a focus for the UK government in 2025 as the reform progresses and takes effect.

Cybersecurity threats and developments

The UK government's Cyber Security Breaches Survey (the "Survey"), published in April 2024, exposed a disconcerting cybersecurity landscape for UK businesses. Approximately 7.78 million cybercrimes were committed against UK businesses in the 12 months prior to the Survey's publication, with half of UK businesses reporting having experienced a cyber-attack or security breach. Phishing attacks emerged as the most common (affecting 84% of businesses), whereas ransomware and denial of service attacks were the least common (affecting 2% or fewer). Nonetheless, the UK's National Cyber Security Centre (NCSC) warned that ransomware posed the most significant threat to UK critical national infrastructure (CNI).

UK businesses and institutions also faced cyberthreats from hostile state actors – including from Russia, China, Iran, and North Korea. These countries exploited the increasingly tense geopolitical situation arising from the conflicts in Ukraine and the Middle East. The NCSC's Annual Review 2024 (the "Review") stated that China presents the most sophisticated cyberthreat to the UK, while Russia encourages non-State malicious actors to launch cyber-attacks against Western countries, alongside its own state-backed cybercampaign.

Ransomware attacks are evolving and – instead of encrypting the stolen data and demanding payment for its decryption – malicious actors are now threatening to publish sensitive personal data online, causing financial and reputational harm to victims. This was the case in the June 2024 ransomware attack on a pathological laboratory service provider to the NHS, which disrupted NHS services and leaked data online. Global ransomware payments totalled USD1 billion in 2023, according to the Review. In May 2024, the NCSC, UK Information Commissioner's Office (ICO) and insurance industry bodies issued a joint guidance, "Guidance for Organisations Considering Payment in Ransomware Incidents", discouraging organisations from making ransom payments.

Technological developments, particularly in AI and quantum computing, also pose a challenge to the UK's cyber-resilience. The Review identified cyber-intrusion as a growing threat in the next five years, facilitated by poor regulation in certain jurisdictions and by AI technological advances that increase the effectiveness of social engineering, vulnerability identification,

and data analysis. This risk is, however, already evident; in May 2024, a deepfake scam resulted in an employee transferring USD25 million to a malicious actor.

The NCSC has warned that the commercialisation of cyber-intrusion tools has made it easier for malicious actors to access and attack systems, and harder to trace them. The NCSC is also cognisant of the impact quantum computing will have on existing cryptography methods and technology in the longer term and urged action to prepare for the emerging cyber-risks.

In 2025, the NCSC is expected to focus on key actions to enhance the UK's cyber-resilience, including:

- promoting basic cybersecurity practices among UK businesses, including a focus on the adoption of the NCSC's Cyber Essentials certification and the Cyber Assessment Framework;
- the publication of more practical guidance from the NCSC and the National Protective Security Authority;
- continued international co-operation and action against malicious cyber actors from hostile states; and
- initiatives to grow a cyberskilled workforce that is cyberliterate and can contribute to cybersecurity technological innovation.

UK cyber-regulation landscape

The UK's cybersecurity landscape underwent significant changes in 2024 and more reforms are expected in 2025.

The Product Security and Telecommunications Infrastructure (PSTI) Act and its accompanying regulations came into force on 29 April 2024. They require organisations that manufacture "relevant connectable products" to meet certain cybersecurity standards such as minimum password requirements, reporting security issues, and minimum periods for which products will receive security updates.

The Labour government, which came to power following the UK's General Election in May 2024, has demonstrated its commitment to cybersecurity reform and progressing the UK's National Cyber Strategy. The King's Speech in July 2024 announced the introduction of two new bills into Parliament – namely, the Cyber Security and Resilience (CSR) Bill and the Data (Use and Access) (DUA) Bill.

The CSR Bill will revise the Network and Information Systems Regulations 2018 (the "NIS Regulations"), which is the only existing sector-wide cybersecurity legislation in the UK. The UK government has been under pressure to update the NIS Regulations – which was implemented pre-Brexit – to align more closely with recent EU legislative developments in this space and, in particular, to expand the scope of the NIS Regulations to include more digital services and supply chains, increase mandatory incident reporting obligations, and provide enhanced powers to regulators. According to the UK Department for Science, Innovation and Technology (DSIT), the CSR Bill will be introduced into Parliament in 2025.

The DUA Bill will amend the existing UK data protection laws. However, owing to the overlap between data protection and cybersecurity, businesses should be aware of the DUA Bill when considering their overall cyber-resilience programme. The DUA has been teased as the potential vehicle for further amendments to the Computer Misuse Act (CMA). Proposed amendments to the CMA were debated in the House

of Lords and subsequently rejected in December 2024 and again in January 2025. The proposed amendments were intended to support cybersecurity professionals that work against cybercrime, included an update to the definition of unauthorised access, and would have provided for a new defence against offences under the CMA where a person is acting to prevent or detect a crime or is otherwise acting in the public interest. The DUA Bill will continue to progress through the legislative process in 2025, most likely without CMA reform. Nevertheless, in October 2024, the UK's Security Minister stated that the Labour government remains committed to tackling cybercriminals ad suggested that a review of the CMA is forthcoming.

In 2024, the DSIT consulted on three draft cybersecurity codes of practice:

- the AI Cyber Security Code of Practice (the "AI COP");
- the Code of Practice for Software Vendors (the "Software Vendors COP"); and
- the Cyber Governance Code of Practice (the "Governance COP").

The AI COP aims to develop a global technical standard for the security of AI systems, based on the principle of "Safety, Security and Robustness" from the UK government's 2023 White Paper, "A pro-innovation approach to AI regulation". The Software Vendors COP sets out four key principles for security measures that businesses that develop and/or sell software in a B2B context should follow, which are:

- secure design and development;
- build environment security;
- secure deployment and maintenance; and
- communication with customers.

The Governance COP outlines five key principles and related actions for good cybergovernance, which relate to risk management, cyberstrategy, people, incident planning and response, and assurance and oversight. The consultations closed in 2024 but the responses have not yet been published. Businesses should keep an eye out for them in 2025.

Finally, in September 2024, the UK government designated data centres as CNI – meaning that, alongside energy supply, water supply and transportation, data centres located in the UK are considered "essential for the functioning of society". As a result, UK data centres can access more support and guidance from the government and the NCSC in the event of outages, cyber-attacks, and adverse weather events.

Supply chain cybersecurity resilience and risk management

Supply chain cybersecurity risk management was a key theme during the course of 2024, particularly in the financial services sector, and this trend is likely to continue in 2025. As businesses become more interconnected, they also become more vulnerable to cyber-attacks through their suppliers, even if they have strong cybersecurity practices themselves.

As mentioned in "UK cyber-regulation landscape", the CSR Bill is expected to expand the scope of the NIS Regulations to (inter alia) introduce new obligations with regard to supply chain management and cyber-resilience – ie, in line with the approach taken in the EU under NIS2 where in-scope entities are required to implement supply chain security policies, supply chain due diligence and minimum supply chain security standards, among other measures. The CSR Bill will likely be scrutinised against NIS2 once published.

In the meantime, the UK has a voluntary approach to supply chain cybersecurity regulation. The Software Vendors COP and the AI COP both include principles and guidance on how to assess and manage supply chain cyber-risks throughout the product life cycle, engage trusted actors involved in the product build and life cycle, and notify vulnerabilities to other parties.

The financial services sector has also made progress in promoting the use of Cyber Essentials, the NCSC-backed scheme that helps organisations improve their cybersecurity and protect themselves from cyber-attacks. Six major UK banks have committed to making Cyber Essentials a requirement for their suppliers and encouraged other businesses to join them. The benefits of this approach include improved supplier due diligence, reduced compliance costs, and improved cyber-insurance coverage across the supply chain.

Additionally, the UK's financial regulators – the Bank of England, the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) – issued a joint policy statement (PS 16/24) on the final Critical Third Party Oversight Regime (the "Regime"), which came into effect on 1 January 2025. The Regime aims to manage the risks to the UK financial system's stability and confidence that could arise from failures or disruptions in the services that a critical third party provides to firms. The Regime consists of several policy statements and rules that apply to third parties that are designated as critical by His Majesty's Treasury. This is similar to the EU's Digital Operational Resilience Act (DORA), which also applies to financial institutions and insurance intermediaries, and which came into effect on 17 January 2025. Under DORA, certain third-party information and communications technology service providers are subject to similar cybersecurity obligations.

Cybersecurity enforcement trends

As it currently stands, the majority of enforcement action concerning cybersecurity in the UK is conducted by the ICO in relation to security incidents under the General Data Protection Regulation (GDPR).

The ICO's report "Data Security Incident Trends" shows that, out of the 60,607 incidents reported to the ICO from the start of 2019 through to the third quarter of 2024, 14,993 (approximately 25%) were cyber-related. There has been a steady number of cyber-incidents reported to the ICO each year, with a slight spike in notifications in 2023 (3,318 in total). As with the findings from the NCSC, the ICO figures show that the most common cyber-incident notifications relate to phishing attacks (approximately 39%), followed by ransomware attacks (approximately 26%) and unauthorised access incidents (approximately 12%).

Despite all the evidence pointing towards a more challenging cybersecurity landscape, as well as the strong signals from the NCSC that cyber-resilience and cyber enforcement are top priorities, the nature of ICO enforcement action appears to have softened. There has been a sharp decline in the number of "investigations" the ICO has launched in response to a notification of a cyber-incident – from 1,497 in 2019 to just 39 in the first three quarters of 2024. However, during the same time period, there has been a steady increase in the "informal action taken" by the ICO. This means that the ICO is increasingly deeming it unnecessary to use its formal powers, such as issuing a fine or a reprimand, and instead provides advice to the notifying organisation.

That said, the ICO is clearly willing to issue fines to organisations that experience a cyber-incident as a result of failing to implement appropriate technical and organisational measures as required under the GDPR, with more than GBP19 million in fines having already being issued in this regard and a GBP6 million provisional fine announced in August 2024. Similarly, the ICO has recently issued reprimands in relation to a variety of cyber-incidents, including a brute-force attack resulting from a known software vulnerability, as well as multiple instances of ransomware attacks, malware attacks, and unauthorised access incidents resulting from non-compliance with GDPR security requirements. It is important to note that, according to the ICO's data protection fining guidance (updated in March 2024), pro-active notification to the NCSC – alongside the usual notification requirements to the ICO – can be considered a mitigating factor by the ICO when deciding to issue a fine.

Taking this in the round, it appears that the ICO's preferred intervention is through the provision of advice and guidance to organisations. Its formal powers seem to be reserved for the most serious failings that lead to a cyber-incident.

Practical considerations

Cyber-attacks pose a serious and growing threat to businesses and institutions in Western countries, requiring more than just compliance measures to protect their assets, data and reputation. Cybersecurity must become a core operational function, with strong leadership and support from the board and senior leaders.

Businesses should assess and address any gaps or weaknesses in their cybersecurity practices, seek accreditation from recognised cybersecurity frameworks where appropriate, and enforce cybersecurity minimum standards across their supply chains. It is critical that employees are provided with adequate cybersecurity training to protect against a successful cyber-attack and to reduce the likelihood of a cybersecurity incident caused by human error or action. Businesses should also monitor the development of new laws and guidance, as well as proactively implement best practice standards as recommended by the NCSC.

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 Rob.Thomson@chambers.com