THOMSON REUTERS
PRACTICAL LAW™

Cybersecurity in the technology sector: issues and challenges

by Eleanor Hobson, Kemp IT Law

Status: **Law stated as at 26-Jun-2024** | Jurisdiction: **United Kingdom**

This document is published by Practical Law and can be found at: **uk.practicallaw.tr.com/w-041-4108**
Request a free trial and demonstration at: **uk.practicallaw.tr.com/about/freetrial**

This note provides a discussion of some of the sector-specific issues and challenges that arise in relation to cybersecurity in the technology sector.

Scope

This note provides a discussion of some of the sector-specific issues and challenges that arise in relation to cybersecurity in the technology sector. This note is focussed on the laws and regulations that apply to the technology sector, being those organisations that specialise in the development and sale of goods and services (including software and cloud services) to fulfil or enable the function of information processing and electronic communications. However, aspects will be relevant for every modern organisation using technology and related services to facilitate or underpin its business operations, and may have particular relevance for those organisations who have transitioned those operations to the cloud.

As the technology sector increasingly underpins and overlaps with other sectors, it is important to note that cybersecurity in the sector is governed by a patchwork of laws, rules, codes of practice and guidelines, both general and specific to this and other sectors. Where a technology sector organisation operates or allows its technology to be used in another sector (for example a regulated sector), that sector may impose requirements that are in addition to or supersede the below. Therefore, to identify the applicable rules and ensure compliance, it is important to review all elements of the organisation's sector, technology, use case(s) and customer base.

For a wider overview of UK cybersecurity law, including those that apply in certain, regulated sectors, see:

- Practice note, UK cybersecurity law.
- Practice note, Cybersecurity in regulated sectors, cybersecurity guidance and standards.

For general information on cybersecurity, see Cybersecurity toolkit.

Cybersecurity risks & compliance

Cybersecurity risks specific to the technology sector

The key cybersecurity risks that have been identified for the technology sector are:

- Heavy reliance on a small number of dominant providers. Having a few dominant providers presents several benefits for cybersecurity, including having substantial budgets to maintain and update the security of their systems. However, it also presents certain risks:
  - These providers underpin critical systems of various parties in supply chains (such as hosting and Software as a service (SaaS) providers). This raises systemic risks, such as if any dominant provider suffers a cybersecurity incident, it may affect other suppliers to any end customers that the dominant provider also underpins. Therefore, any compromise of the dominant provider can present a 'single point of weakness' for attacks (see DSIT: Research on UK managed service providers). See, for example, the National Cybersecurity Centre joint announcement with the Republic of Korea on DPRK-sponsored cyber attacks on software supply chains (NCSC: UK and Republic of Korea issue warning about DPRK state-linked cyber actors attacking software supply chains), or the 2017 NotPetya attack that exploited a Ukrainian accounting software business and resulted in significant global damage estimated at 10 billion USD (see Article, Ransomware cyber attacks: lessons learned at last?);
  - The dominance of these providers means it's unlikely that customers (even large or influential ones) will be able to negotiate any deviations from a provider's supplier standard terms to protect

particularly sensitive or critical data or systems. See, for example, the German data protection regulators' negotiations with Microsoft on their data protection agreement, which the regulators reported resulted in "only ... minor improvements in the[ir] points of criticism" (see DSK: AG DSK „Microsoft-Onlinedienste").

- Other supply chain risks, particularly for complex sub-processing chains. These include an increased attack area to an organisation's systems, external storage of or access to the organisation's systems and data (over which they may have limited control) and cyberattacks or malware originating from the supplier. Technology providers increasingly rely on a large number of outsourced, subcontracted or interconnected services. Therefore, it can be difficult for them and their customers to map their supply chains, fully assess and identify their cybersecurity risks and implement appropriate security measures. For example, the Department for Science Innovation and Technology (DSIT), in its 2023 call for views on software resilience and security for business operations, reported a 742% average annual increase in software supply chain attacks between 2019 and 2022. However, the UK's 2024 Security Breaches Survey noted that only 11% of businesses review supply chain risks posed by their immediate suppliers and 6% look at the wider supply chain. (Although these increase for large enterprises, the figures remain low at 48% and 23%) The interdependency between technology businesses can also result in circular supply chains where organisations act as both as customer and supplier for each other, exacerbating the problem. For more information, see:
  - Legal update, Government launches call for views on software resilience and security for business organisations.
  - DSIT: Cyber security breaches survey 2024.
- Failures of critical systems. A technology failure can affect national security or systems critical to society or to life, such as critical national infrastructure and medical devices.
- Global reliance on systems, requiring high availability. For example, a multinational customer may require a system to be available constantly, from multiple jurisdictions in multiple time zones. This can make it difficult to track and detect cyberattacks.
- Increasing use of artificial intelligence (AI). As for all its use cases, AI can be very helpful in detecting, mitigating and preventing cybersecurity risks and attacks. However, its growth, particularly in relation to Generative AI, can also pose increased cybersecurity risks:
  - By attackers. Attackers may use AI to enhance or increase their attacks on technology (and, accordingly, on those organisations providing and using that technology) for example, through more sophisticated or voluminous malware, social engineering and open source intelligence (OSINT);
  - By suppliers. Technology providers re-using public or customer data to train their (or another party's) AI can cause confidential data leakage. Vendors operating on or through a third party system can also cause accidental risks such as introducing vulnerabilities, sharing privileged access credentials and misuse of application programming interfaces (APIs).
- Potential for misuse. The prevalence of Internet of Things (IoT) devices can allow for intrusive or unlawful surveillance, malicious interference or unauthorised collection of information if the device is not properly patched and maintained, or if embedded security measures are weak or non-existent.
- State-sponsored attacks. States are increasingly exploiting all layers of the tech stack to launch state-sponsored attacks, often with devastating consequences for the target, as well as for other untargeted organisations who may get caught in the consequences of an attack. For example, the NotPetya attack.

These risks are regulated or managed under a patchwork of legislation, case law, regulatory guidance, codes of practice and policy (see Regulations, legislative and regulatory frameworks, codes and voluntary guidelines.)

More generally, the UK government annually conducts and publishes the Cyber Security Breaches Survey and Cyber Security Longitudinal Survey, which it uses to inform policy, and can be a helpful reference for trends in cyber practices, risks, incidents and costs (see, for example, DSIT: Cyber security breaches survey 2024 and DSIT: Cyber security longitudinal survey: wave three results).

For an outline of the common cybersecurity threats to businesses and common failures by business that may lead to security breaches, see Cyber threats toolkit (Sectors).

Practical steps to mitigate cybersecurity risks

Some examples of practical steps entities operating in the sector can take to mitigate cybersecurity risks are:

- Identifying and understanding its regulatory responsibilities and any minimum security requirements imposed under law (see Regulations, legislative and regulatory frameworks, codes and voluntary guidelines) and undertaking cyber risk assessments in light of these regulatory requirements,

considering the organisation's specific IT and OT assets, operations and organisational structures and the cyber risks present and prevalent in the sector (see Practice note, Cybersecurity risk assessments and reporting (UK)).

- Escalating cybersecurity to a board or management level risk item.
- Updating and maintaining an enhanced information security programme, including:
  - Appropriately and regularly testing Incident Response, Business Continuity and Disaster Recovery plans, including appropriate redundancy, back-ups, recovery time objectives (RTOs), recovery point objectives (RPOs), and penetration testing;
  - Encrypting data at rest, in transit, and (where practicable) in motion;
  - Promptly patching and maintaining systems and software;
  - Implementing least privilege access rights;
  - Using security incident event monitoring systems (SIEM) and other security software, monitoring and reporting;
  - Management of all devices and hardware, including updates and maintenance, acceptable use policies and prohibiting use of portable media (such as USBs);
  - Other technical and organisational measures, for example two or multi-factor authentication and controls on staff access to third party websites and systems; and
  - Promptly notifying (as appropriate) and investigating information security breaches.

  For more information on the types of policies and procedures an organisation might want to adopt as part of an enhanced information security programme, see Practice note, Cyber risk roadmap.
- For service providers (and their supply chains):
  - Undertaking due diligence before and periodically during their engagement (see Practice note, Managing cybersecurity risk in supplier relationships (UK) and Standard document, Cyber due diligence questionnaire for suppliers (UK)).
  - Flowing down the above security standards (as appropriate to the service).
  - Adding supplier risks to risk registers.
  - Undertaking detailed supplier and data flow mapping.
- Adhering to national and international security guidance, standards, audits, reporting and certifications, including ISO 27001, SOC 2, and the UK's Cyber Essentials scheme (see Practice note, Demystifying cybersecurity industry standards and certification schemes (UK)). In addition, the NCSC also operates a certification program where products, organisations, services and training can be certified as meeting certain industry requirements (see NCSC: Products and services, NCSC certification).
- Regular (at least annual) cybersecurity training to staff members, and simulating attacks, such as test 'phishing' emails and OSINT reviews.
- Producing standardised cybersecurity contractual terms or requirements for the entity's business.
- Taking out appropriate cyber insurance (see Practice note, Cyber insurance: an overview).

For more information on managing cybersecurity risks, see Toolkit, Cybersecurity toolkit: Managing cybersecurity risks and threats.

Main challenges in relation to mitigating cybersecurity risks

An organisation's chosen cybersecurity measures will depend on the specific activities of the organisation, the sectors in which it and its customers operate, the risks inherent in such operations and (as far as contractual commitments go) its commercial bargaining power.

Key challenges in the technology sector often include:

- Maintaining sufficient stakeholder and staff member engagement to ensure a comprehensive cybersecurity programme is budgeted for, implemented, tested and regularly updated.
- Tackling human error risks, which are (to a certain degree) outside of the organisation's control.
- For technology providers operating a "one to many" service (for example multi-tenancy SaaS), maintaining standard technical security controls across their customer base, while accommodating bespoke customer security requirements. On this point, multi-tenant architecture typically presents more cybersecurity risk when compared to single-tenant architecture. For more information, see Practice note, Cloud services: hybrid cloud and outsourcing: Shared or dedicated infrastructure and Multi-tenancy or single tenancy.
- Reliance on dominant technology providers in the technology stack, thereby limiting the security measures and contractual commitments available.
- Complex supply chains making it difficult to map data flows and identify relevant risks.
- Evolving security measures to keep on top of new and developing risks, such as vulnerabilities, patching and novel risks presented by AI and (one day) quantum computing. (For more on vulnerability management, generally, see Cyber vulnerability management toolkit (Sectors).)

- Increasing premiums for and exclusions under cyber insurance policies that leave organisations without adequate protection for losses. Certain losses may also not be recoverable as a matter of public policy, such as regulatory fines. (See Practice note, Cyber insurance: an overview).

Regulation and guidance

Sector-specific UK policy considerations

The UK government set out its ambitions for the UK to become a science and technology 'superpower' by 2030 in the Digital Strategy 2022 and Science and Technology Framework 2023, which built on many existing technology sector commitments and initiatives, including in relation to cybersecurity. This also overlapped with the government's ambition for the UK to be one of the world's leading democratic cyber powers (see Cabinet Office: The Integrated Review 2021, p7).

The UK government's "£2.6 billion" National Cyber Security Strategy was published in 2021 and updated in 2022. It is reported against by the government on an annual basis. It is built around five pillars of strengthening the UK's cyber ecosystem, building resilience, investing in technology, advancing global leadership, and disrupting the UK's adversaries in cyberspace (see Legal update, Government publishes new National Cyber Strategy).

Initiatives under this strategy include the National Security Strategic Investment Fund for venture capital investment in dual-use technologies including cybersecurity, the Cyber Runway accelerator programme for cyber entrepreneurs and start-ups, the CyberFirst education and bursary scheme for engaging and training youth talent, and the Digital Security by Design programme (in partnership with industry) to support the development of more resilient digital infrastructure. The government also annually publishes a Cyber Security Sectoral Analysis report on the UK's cybersecurity industry, including size, employment and revenue.

Alongside these initiatives, in 2023 DSIT issued a call for views on software resilience and security for businesses and organisations. DSIT published its response to that call for views in early 2024, including its plans to develop a package of policy interventions:

- A new statutory framework and regulatory function for UK-based data centre services, a consultation on which was published in December 2023 and open until February 2024 (see Legal update, Government consults on minimum security standards for data centres). The proposed framework follows a 2022 call for views and would apply to operators of third party data centres, particularly those providing colocation or co-hosting data centres, requiring them to register with and report significant incidents to an (as yet unconfirmed) regulator, and apply a set of minimum standards for security, assurance and testing.
- A Cyber Governance Code of Practice, a draft of which was published in January 2024 for consultation until March 2024. This Code would be (at least initially) voluntary for directors of all organisations to monitor and manage their business' cyber risks, together with a potential assurance mechanism (see Legal update, Call for views launched: government seeks feedback on draft Cyber Governance Code of Practice).
- A Code of Practice for Software Vendors, a draft of which was published in May 2024 (see Legal update, Government launches call for views on code of practice for software vendors). The current draft suggests that the Code would be (at least initially) voluntary and cover B2B developers, resellers and distributors of software products and services (including SaaS and other cloud services) and products and services that contain software (for example IoT devices and managed services providers). Open source developers may also find aspects useful. The Code is intended to set "clear baseline expectations" for software security, for customers (including government) to use in procurement.
- A Code of Practice for Cyber Security of AI, a draft of which was published in May 2024, together with a series of supporting research reports (see Legal update, Government launches call for views on code of practice for AI cybersecurity). The Code is based on the NCSC's 2023 guidelines for secure AI system development, and is relevant for all AI supply chain stakeholders, with a particular focus on developers and system operators.
- A series of measures designed to strengthen accountability in the software supply chain by producing standardised procurement clauses, cybersecurity training for UK procurement professionals, content on using Software Bills of Materials (software ingredients lists) and possibly introducing new accreditations. For example, the establishment of the UK Cyber Security Council (UK Cyber Security Council) and the adoption of their published professional standards for cybersecurity professionals, with a pilot programme offering chartered status for cybersecurity professionals (see DSIT: Statement from HM Government on the adoption of UK Cyber Security Council standards and UK Cyber Security Council: About Professional Standards and Professional Registration).

Other technology sector initiatives also have a focus on cybersecurity, such as the government's new Frontier AI Taskforce, whose first priority is considering the role of AI in national security, the National Cyber Advisory

Board (of academia, industry and third sector groups), and the government's consultations on updating:

- The Network and Information Systems (NIS) Regulations 2018 (NIS Regulations) including to broaden the types of IT organisation that are subject to its minimum cybersecurity requirements.
- The Computer Misuse Act 1990, which may establish defences for 'white hat' hacking for research or the public interest.

The Joint Committee on the National Security Strategy has published Special Reports and Responses on its Inquiry into Ransomware, which launched in October 2022 (see UK Parliament: Committees: Ransomware).

For further information on UK proposed cybersecurity reform which will impact the technology sector, see Practice note, Managing cybersecurity risk in supplier relationships (UK) and, in particular, Future regulation of digital supply chains

Regulations, legislative and regulatory frameworks, codes and voluntary guidelines

A patchwork of legislation, case law, regulatory guidance, codes of practice and policy regulates and manages various aspects of cybersecurity in the technology sector, including:

- The NIS Regulations which require in-scope organisations to implement appropriate and proportionate technical and organisational measures (APTOMs) to prevent and minimise the impact of incidents on network and information systems (NIS), and to report incidents to the ICO, or other sector-specific competent regulators or the NCSC (see Regulators and enforcement). The NIS Regulations apply to relevant digital service providers (RDSPs) (namely online marketplaces, cloud computing providers and search engines which meet specified criteria) as well as operators of essential services (OESs) in specific sectors, including technology-related sectors such as digital infrastructure. The government is proposing to expand the scope of the NIS Regulations in future to cover managed services providers, recognising the crucial functions these organisations play as part of vital supply chains (see Practice note, Cybersecurity Directive: UK implementation: Future, planned reform). The ICO has also produced specific guidance on security measures for RDSPs (see ICO: Security requirements).
- Technology sub-sector specific laws, regulations and codes of practice for connected devices, such as:
  - the Connected Electric Vehicles (Smart Charge Points) Regulations 2021,
  - NHS Data Security Centre guidance and policies for NHS patient data systems and connected medical devices,
  - the voluntary code of practice on improving the security and privacy of apps and app stores (see Legal update, Government makes changes to voluntary code of practice for app store operators and developers and extends implementation period); and
  - the Product Security and Telecommunications Infrastructure Act 2022 (PSTIA), which imposes minimum security requirements on certain in-scope IoT devices (see Practice note, Cybersecurity requirements for consumer connectable products under Part 1 of Product Security and Telecommunications Infrastructure Act 2022 (UK)).
- The UK GDPR which requires controllers to implement APTOMs to prevent any compromise of personal data, and report certain incidents to the ICO, controllers and affected individuals.
- The Privacy and Electronic Communications (EC) Regulations 2003 (PECR) and Communications Act 2003 which requires public electronic communications service providers to secure their systems and notify the ICO and/or OFCOM of certain security breaches.
- Other sector-specific regulation and guidance, requiring cybersecurity measures and the flow down of those measures, including contractual terms, to their technology providers, or that catch XTechs (for example, financial entities under the FCA Handbook, and manufacturers of medical devices under the Medical Devices Regulations 2002 and General Product Safety Regulations 2005). For more information, see Practice note, Cybersecurity in regulated sectors, cybersecurity guidance and standards.
- Computer Misuse Act 1990, including offences for intentionally obtaining unauthorised access to, impairing the operation of, or preventing or hindering access to any program or data held in a computer, enabling another to do so, or supplying any article to do so.
- Other criminal legislation, including the Fraud Act 2006 and Theft Act 1990 that might apply to cyberattacks involving phishing emails or ransomware.
- Laws relating to an organisation's vicarious liability for its employees for cybersecurity incidents caused by human error or disgruntled employees. (See, for example, Practice note, UK cybersecurity law: Vicarious liability).
- Other developing Codes of Practice, UK Cyber Security Council professional standards and other measures,

for technology businesses and their customers (see Sector-specific UK policy considerations).

- NCSC guidance, infographics and advice on cybersecurity, including its supply chain security and mapping guidance (NCSC: Guidance: Supply chain), Cyber Security Toolkit for Boards (NCSC: Cyber Security Toolkit for Boards) and Cloud Security Guidance on how to choose, configure and use cloud services securely (NCSC: Cloud security guidance).

Organisations should be mindful that some of the above requirements may apply to the organisation's group as a whole or have extra-territorial effect. For example, under UK GDPR, relevant obligations can apply to multiple group entities involved in a processing chain (UK and non-UK) and fines may be calculated with reference to global groupwide turnover.

As noted above, as the technology sector increasingly underpins and overlaps with other sectors, where a technology sector organisation operates or allows their technology to be used in another sector (such as by financial, legal and healthcare service providers, public companies and public sector organisations), that sector may impose requirements that are in addition to or supersede the requirements outlined in this note. Therefore, to identify all applicable rules and ensure compliance, it is important to review all elements of the organisation's sector, technology, use case(s) and customer base. See Practice note, Cybersecurity in regulated sectors, cybersecurity guidance and standards.

Regulation of critical infrastructure, essential and digital services

There are 13 UK national infrastructure sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water.

According to the National Protective Security Authority (NPSA), Critical National Infrastructure (CNI) are:

> "[t]he elements of national infrastructure the loss or compromise of which could result in major detrimental impact on essential services, significant loss of life or casualties, significant economic or social impacts, or have a significant impact on national security, national defence, or the functioning of the state."

*(*NPSA: Critical National Infrastructure*).*

Technology sector organisations will be captured where they provide systems that fall within this definition or underpin others that do.

CNI operators are subject to specific security guidance from their Lead Government Department, the National Cybersecurity Centre (NCSC), the NPSA and other national security authorities. For example, users and providers of cyber components of CNI physical security systems are subject to the NPSA's Cyber Assurance of Physical Security Systems (CAPSS) Standard and Guidance.

The NIS Regulations also impose obligations on OESs and RDSPs. As mentioned in Regulations, legislative and regulatory frameworks, codes and voluntary guidelines, OESs are organisations providing services essential to critical societal or economic activities that are reliant on network and information systems (NIS), where any incident would significantly disrupt that service, and RDSPs are providers of UK information society services of online marketplaces, cloud computing providers and search engines, subject to some exemptions.

OESs' and RDSPs' obligations include to implement APTOMs to prevent and minimise the impact of incidents on their NIS, and to report incidents to their designated competent authority and/or NCSC. OESs are regulated by their sector-specific authority, while RDSPs are regulated by the ICO.

For more information, see Practice note, Cybersecurity Directive: UK implementation.

Regulators and enforcement

Regulators relevant to cybersecurity in the sector

Several regulators have competence for matters which cover cyber incidents and cybersecurity in the UK, according to the subject matter of the breach, the sector and/or the affected product or service.

Key regulators for cybersecurity in the UK technology sector include:

- The ICO. The ICO is the UK's independent data protection authority responsible for enforcing UK data protection, privacy and freedom of information laws. It is also the designated competent authority for RDSPs under the NIS Regulations and can bring prosecutions under the Computer Misuse Act 1990. All personal data breaches reportable under the UK GDPR should be reported to the ICO. The NIS Regulations also require RDSPs to notify the ICO of any cybersecurity incident that has a substantial impact on their services.
- The Office of Communications (OFCOM) which is the competent authority for the digital infrastructure sector under the NIS Regulations. Public electronic communications service providers must also notify the ICO and/or OFCOM of security breaches under

the Privacy and Electronic Communications (EC) Regulations 2003 and Communications Act 2003.

- The Office for Product Safety and Standards (OPSS), which has been appointed to enforce the PSTIA, which imposes minimum cybersecurity requirements on manufacturers, distributors and importers of in-scope IoT devices. The OPSS is the national enforcement authority for all consumer products, and enforces a wide range of product regulation covering products that also fall in scope of the PSTIA regime.

Generally, cyber incidents should also be reported to the NCSC, which operates across sectors. Although the NCSC is not a regulatory or law enforcement body, it can provide guidance and support to businesses. It also monitors for systemic cybersecurity risks or attacks and will also coordinate and lead any associated response of relevant government entities.

Technology businesses operating or providing products or services to regulated sectors may need to notify or cooperate with their customers in notifying regulators in those sectors, such as the Financial Conduct Authority (FCA), Civil Aviation Authority (CAA), Medicines and Healthcare products Regulatory Agency (MHRA), or Office for Product Safety and Standards (OPSS).

If a technology business suspects a cyber incident relates to criminal activity, they should also report the incident to law enforcement. (It's worth noting that making ransomware payments can attract criminal liability, for example under money laundering, sanctions, proceeds of crime or terrorist financing law.)

For more information on cyber regulators and advisory bodies, generally, see Practice note, Cybersecurity regulators and advisory bodies. For more information on notification requirements, see Practice note, Security incident notification requirements (UK).

Scope of responsibilities

The NCSC is the main UK cybersecurity-specific public body and operates across sectors. It is not a regulator, and so does it not have any express enforcement powers but does provide public guidance, coordinate national cyber incident responses, support academic and industry expertise, and assist in securing national infrastructure.

In the UK regulators are generally given a broad remit and therefore generally have a range of other responsibilities in addition to cybersecurity. Some regulators have been appointed to regulate cybersecurity for one specific industry sector only (such as the FCA in respect of financial services) while others have remit to cover a range of matters (including cyber) across multiple industry sectors, which may include the technology sector. In some cases, a regulator will be tasked with a hybrid of sector-specific and cross-sector regulation.

For example, the ICO regulates personal data and other related privacy and digital matters, including direct marketing, cookies and freedom of information across multiple sectors, and these matters will often involve an assessment an organisation's cybersecurity posture and any data breaches. However, with respect to cybersecurity under the NIS Regulations, the ICO's regulatory scope is limited to ex post oversight of certain, qualifying digital service providers only. By way of another example, OFCOM is responsible for all communications services matters, including broadband, television, radio and the postal service.

Sector-specific regulators, like the FCA, are generally responsible for all matters related to the organisations they regulate, including for receiving reports of cybersecurity incidents and regulatory action for inadequate preventative measures. However, some other sector-specific regulators may have delegated bodies to manage the cybersecurity risks in that sector, for example, NHS England has set up the NHS Data Security Centre (NHS DSC).

Main powers of the sector regulator and funding

As discussed above, multiple regulators may operate in the technology sector, each with their own powers set out in their respective mandates.

By way of example (in relation to cybersecurity under the UK GDPR and DPA, PECR and NIS Regulations) the ICO can:

- Produce relevant codes of practice, guidance and advice.
- Establish, support and oversee certification mechanisms and codes of conduct.
- Require an organisation to provide the ICO with information (sometimes within 24 hours).
- Require an organisation to notify an affected individual of a data breach.
- Conduct audits, assessments and inspections (sometimes without notice).
- Issue warnings and reprimands.
- Issue enforcement notices requiring an organisation to take remedial steps (sometimes within 24 hours).
- Administer fixed penalties and maximum fines of up to: (i) £17 million (NIS Regulations), (ii) the greater of £17.5 million or 4% of global annual turnover (UK GDPR and DPA), or (iii) £500,000 (PECR).
- Apply for a court order to enforce any of the above.
- Prosecute relevant criminal offences before the courts.

UK regulators, as public bodies, are generally funded by a combination of UK government funds, fees charged to

their regulated firms and a proportion of the regulatory fines they recover.

For example, the ICO reports that it is predominantly (approximately 85%, see ICO: How we are funded) funded by payment of the data protection fee by personal data controllers at registration. The remaining funds are granted by the UK Government or received as a proportion of the fines they've recovered (up to a maximum of £7.5 million).

Approach to enforcement

Each regulator has their own approach to enforcement. Often, this will depend on their published regulatory policies.

The ICO is generally seen as taking a collegial approach to regulation and enforcement. The ICO generally likes to see that organisations have taken steps to consider their cybersecurity risks, and adopted preventative measures that are appropriate to their activities, systems and data. Regulatory action is likely to be harsher if the organisation has negligently or deliberately decided not to seek advice, implement appropriate measures or report an incident to the ICO or the NCSC (or others).

For example, in the ICO's document outlining how it intends to exercise its powers in the context of its new strategic plan (see ICO25 – Our regulatory approach) the ICO states that:

> "[W]hen selecting the right regulatory response to an incident or possible breach, we will consider carefully and recognise steps that an organisation has taken to comply with its obligations. This includes the advice it may have taken on measures to avoid a security breach. For example, whether it has sought advice from a professional recognised by the UK Cyber Security Council, the [NCSC], or other equivalent organisation. As well as the practical steps it has implemented (such as obtaining certification through the government-backed Cyber Essentials scheme or by complying with another similar code or certification scheme)."

Under their MoU with the NCSC, the ICO committed to explore how to demonstrate that meaningful engagement with the NCSC will reduce regulatory penalties (see NCSC: NCSC CEO and Information Commissioner sign Memorandum of Understanding).

For more information, generally, on the ICO's approach to enforcement, see Practice note, Maintaining a transparent and constructive relationship with the Information Commissioner's Office (ICO).

Collaboration and information sharing between regulators

There are frameworks in place supporting collaboration between the regulators may operate in the technology sector.

Public sector bodies often enter into MoUs or other agreements with one another to govern their responsibilities, co-operation and information sharing where they both have competency in relation to an incident. For example, the ICO and NCSC recently signed an MoU on their cooperation and information sharing, including to mutually agree press releases, cooperate on guidance and coordinate engagements with organisations suffering data breaches to minimise disruption, see Legal update, Information Commissioner and National Cyber Security Centre CEO sign Memorandum of Understanding.

The ICO also has MoUs with several other UK and international authorities to share sensitive and confidential information, including the FCA, the Home Office, the Intelligence Community, the Insurance Fraud Bureau, the National Data Guardian, the UK Regulators Network, other international data protection regulators, and the US Federal Trade Commission (see ICO: working with other bodies).

The ICO may also share data with law enforcement agencies where relevant.

The NCSC also works with other authorities, according to the type of cybersecurity incident. For example, the NCSC may liaise with the NPSA, Cabinet Office and relevant Lead Government Departments (the government departments designated by the Cabinet Office to manage certain emergency situations, including emergency planning) for cybersecurity incidents affecting critical national infrastructure.

For technology businesses operating or providing services to customers across other sectors, information may be similarly shared by their competent regulator. For example, if a cybersecurity event resulted in a major operational disruption to the UK's financial sector, the UK financial authorities will co-ordinate under the Authorities' Response Framework and share information with the NCSC and other government bodies. Where a breach impacts an OES or RDSP under the NIS Regulations then a framework for information sharing between the NIS enforcement authorities, relevant law-enforcement authorities, the NCSC and (where appropriate) public authorities in the EU is set out in the regulations.

However, this does not mean that all information will be shared by all relevant parties. Information shared with some authorities may be kept confidential, while others

may publish the information they receive, or otherwise be obliged to do so (for example in response to freedom of information requests or due to a regulatory requirement). For example, notifications to the NCSC will not generally be passed to the ICO without the notifying organisation's consent, although they will share other information, such as on cyber threats likely to affect national infrastructure or security, RDSPs and other organisations.

Organisations should ensure they are aware of who their relevant competent authorities are in the event of an incident, and what their notification obligations are under law, and keep track of the information provided to each.

History of enforcement actions in this sector

In 2022, the ICO fined two businesses, Tuckers Solicitors (£98,000) and Interserve Group (£4.4million) under the UK GDPR for failing to implement appropriate cybersecurity measures, including a process for regular patching of vulnerabilities (see Practice note, ICO civil penalties: tracker).

However, more recently, ICO enforcement seems to have shifted from imposing monetary penalties to issuing reprimands. The ICO announced this change for public sector entities in 2022, however, it also appears to be a trend in enforcement against private sector entities (such as the use of reprimands against My Media World Limited t/a Brand New Tube and Gain Capital UK).

In 2023, the ICO also announced its investigations into a number of high profile public sector personal data breaches although, as at the time of writing, no enforcement action has been taken.

The ICO came under pressure after a January 2023 public announcement that they had decided to stop enforcing personal data breach reports made by communication service providers under Regulation 5A of PECR. The page was subsequently removed, however, whether the ICO's position has (informally) changed is unclear.

As noted above, technology sector organisations may be subject to supervision by other regulators, such as the FCA, who may take enforcement action in addition to any regulatory action by the ICO. For example, the FCA fined Equifax £11.1 million (reduced from £15.9 million due to settlement) in October 2023 in relation to a 2017 cybersecurity incident affecting UK consumer data transferred to its parent company Equifax, Inc. (see Legal update, FCA fines Equifax Ltd for cyber security and outsourcing failings).

In addition, the ICO, itself, has remit to fine organisations for breaches of different legal cybersecurity requirements, which may or may not overlap (for example, action may be taken against an in-scope technology company for a breach of the UK GDPR, the NIS Regulations and/or the PECR).

It is worth noting that it can take some time to complete the regulatory review. For example, the above Equifax fine by the FCA related to a 2017 data breach, and Gain Capital UK reported the personal data breach in April 2020 that led to its ICO reprimand in March 2023 (see *ICO: Gain Capital UK Limited*).

As above, organisations should be mindful that some cybersecurity requirements may apply to the organisation's group as a whole or have extra-territorial effect. For example, the FCA fine of Equifax (noted above) related to activities of the UK entity's US parent.

Public reporting of cyber incidents

All enforcement notices and decisions of the ICO are published on the ICO's website and generally announced via press release by the ICO. The ICO also lists all personal data breaches reported to or investigated by the ICO in their "Complaints and concerns data sets" on a quarterly basis. If the cyber incident has resulted in a personal data breach that is likely to result in a high risk to affected individuals, then the organisation will need to notify affected individuals (who may circulate that information). See ICO: Enforcement.

Cyber incidents reported to the NCSC are treated as confidential and are not generally shared with the ICO without the organisation's consent, although information sharing provisions exist under the NIS Regulations with respect to incidents that fall under the scope of those regulations, and information may be shared with law enforcement bodies (see Collaboration and information sharing between regulators). In addition, the NIS Regulations provide powers to competent authorities and the NCSC to make the public aware of incidents impacting OESs and RDSPs, subject to rules set out in the regulations. This will normally be done only after a period of consultation with the relevant OES or RDSP.

Other sector-specific authorities may share and publish information where they deem appropriate. For example, NHS organisations are notified of cyber security threats through the NHS Cyber Alert service, which are then published online.

Some organisations may choose to publish information relating to a cyber incident where it is likely the circumstances will otherwise be publicly reported or shared.

Where technology organisations are obliged to report cyber incidents to their customers, it's worth noting that

they may be limited in their control over the information that is publicly released. For example, under UK GDPR where they act as a processor on behalf of a customer acting as controller of personal data affected by a cyber incident, although the organisation may not be required to, their customers may be required to share or publish information as set out above.

Liability for cybersecurity incidents

There is a general acceptance that cyber incidents are a 'when' rather than 'if' event. See, for example, Article, A question of 'when' and not 'if': protecting your organisation from cyber attacks in 2018.

Not all cyber incidents will amount to a breach of law or obligation (contractual or otherwise) or incur liability to third parties. For example, an organisation may take all appropriate security measures, but still be subject to a malicious or state-sponsored attack.

However, possible liabilities may include:

- Regulatory fines from the ICO, which could be issued under a number of different pieces of legislation that may apply to an organisation in the tech sector. For example, fines may be issued under the UK GDPR if the breach reveals that the organisation didn't take appropriate steps to protect its personal data from a cyber incident. For example, not encrypting data at rest, failing to patch or update systems, inappropriate access privileges, or over-retention of personal data.
- Other non-monetary regulatory action, such as public reprimands and enforcement notices requiring the organisation to take certain steps.
- If the organisation operates in another regulated sector (for example financial services or one of the sectors regulated under the NIS Regulations), it may be subject to other regulatory action, including fines, enforcement notices and adjustments to or loss of authorisations. See Practice note, Cybersecurity in regulated sectors, cybersecurity guidance and standards.
- Follow-on claims from other affected parties, including customers and data subjects, and representative actions. These may include breach of contract, confidence, trust, or intellectual property rights, negligence or compensation associated with loss of the data. For a brief summary of some other civil actions that might arise following a data breach, see Practice note, UK cybersecurity law: Civil actions. Under the UK GDPR all organisations involved in the processing are jointly and severally liable for any infringement of UK GDPR, unless they can show they were not in any way responsible for the event giving rise to the damage (*Art.82(3), UK GDPR*).
- Costs associated with investigations and reports, cooperation with regulators and other affected parties, remediation, business continuity and disaster recovery (including procuring alternative systems, restoration from back-ups, employee and management time), legal and other advisory costs.
- Ongoing monitoring costs for the organisation and affected third parties (including publication or auction of stolen data, further attacks, subscriptions for credit or other identity theft monitoring services).
- Losses associated with termination of customer contracts, such as for material breach.
- Reputational damage and loss of goodwill.
- Higher premiums for cyber (and related) insurance.

Where the organisation operates in or services customers in other countries, the organisation may also be subject to liabilities in those other jurisdictions. For example, UK organisations servicing EU consumers may also be subject to fines under EU GDPR. For more on the EU GDPR, see Practice note, Overview of EU General Data Protection Regulation.

It is worth noting that the ICO has stated in its MoU with the NCSC that it "looks favourably on victims of nationally significant cyber incidents who report to and engage with the NCSC", and this active engagement with the ICO and NCSC may result in reduced regulatory fines (see ICO: Memorandum of Understanding with NCSC).

Approach to enforcement

Each regulator has their own approach to enforcement. Often, this will depend on their published regulatory policies.

The ICO is generally seen as taking a collegial approach to regulation and enforcement. The ICO generally likes to see that organisations have taken steps to consider their cybersecurity risks, and adopted preventative measures that are appropriate to their activities, systems and data. Regulatory action is likely to be harsher if the organisation has negligently or deliberately decided not to seek advice, implement appropriate measures or report an incident to the ICO or the NCSC (or others).

For example, in the ICO's document outlining how it intends to exercise its powers in the context of its new strategic plan (see ICO25 – Our regulatory approach) the ICO states that:

> "[W]hen selecting the right regulatory response to an incident or possible breach, we will consider carefully and recognise steps that an organisation has taken to comply with its obligations. This includes the advice it may have taken on measures to avoid a security breach. For example, whether it has sought advice from a professional recognised

by the UK Cyber Security Council, the [NCSC], or other equivalent organisation. As well as the practical steps it has implemented (such as obtaining certification through the government-backed Cyber Essentials scheme or by complying with another similar code or certification scheme)."

Under their memoranda of understanding (MoUs) with the NCSC, the ICO committed to explore how to demonstrate that meaningful engagement with the NCSC will reduce regulatory penalties (see NCSC: NCSC CEO and Information Commissioner sign Memorandum of Understanding).

For more information, generally, on the ICO's approach to enforcement, see Practice note, Maintaining a transparent and constructive relationship with the Information Commissioner's Office (ICO).

Cybersecurity issues in relation to engaging with third parties

Cybersecurity due diligence on third party suppliers or contractors

The scope of cybersecurity due diligence for customers in the technology sector on a supplier or contractor will depend on the nature of the services to be provided, and the extent of its access to the organisation's and its customers' systems and data. However, it should be expected that customers in the technology sector will be technically savvy and that the goods and services they are likely to procure from other technology-sector organisations will be technologically complex.

Bearing that in mind, frequent due diligence steps include:

- Completion of questionnaires on the provider's information security programme.
- Confirmation that the provider is certified under any relevant national or international standards (for example, ISO27001, Cyber Essentials and NCSC certification).
- Requesting copies (or summaries) of any penetration tests and security reports (for example, System and Organisation Controls (SOC) 2).
- Information on the provider's support, maintenance, business continuity and disaster recovery measures. If the provider will be providing Anything as a Service (XaaS), storing any data or responsible for hosting, these should include updates, patching, SLAs, service credit redundancy, back-ups, RTOs and RPOs.
- If the provider will be storing or hosting data, whether the hosting is subcontracted (and if so, to whom and where), and which encryption measures are applied, including whether they apply at rest, in transit or in motion, who has access to the keys and any 'bring your own key' functionality.
- The scope of the provider's access to the organisation's data and systems, including any controls the organisation has on that access.
- The locations from which the services will be provided.
- Any sub-contracting arrangements (including any of the above information on those) and whether the organisation has any control over their appointment.
- Contractual protections, including incident reporting and remediation commitments.
- Insurance coverage.
- General internet searches in case of any public disputes, breaches or enforcement action.

For more on due diligence generally, see Standard document, Cyber due diligence questionnaire for suppliers (UK).

Key issues and practicalities to consider

Key steps for technology sector businesses to take in relation to cybersecurity prior to engaging suppliers, subcontractors and customers include:

- Mapping their own systems and data flows, including identifying critical systems, sensitive data, third party access, access rights, and any international data flows or access.
- Formalising their internal cyber security policy, including their relevant commitments under law, for example, incident response, reporting and APTOMs under NIS Regulations and UK GDPR, sector-specific requirements, and their standard or minimum commitments to/from customers and suppliers. (See Cybersecurity due diligence on third party suppliers or contractors for considerations). See also Practical steps to mitigate cybersecurity risks.
- Preparing a standard customer-facing cybersecurity policy and standard contractual terms.
- Establishing a process for logging any deviations from their standard cybersecurity terms for customers and suppliers. For example, the large hosting providers are unlikely to accept bespoke terms, and some customers may request the organisation complies with their own information security policies.
- Compiling a standardised cybersecurity questionnaire (or section of the general supplier questionnaire) that includes a process for assessing the supplier against the above. See, for example, Standard document, Cyber due diligence questionnaire for suppliers (UK).
- Assessing whether any certification (such as ISO27001) would be appropriate for the business. See Practice

note, Demystifying cybersecurity industry standards and certification schemes (UK).

- Implementing a program of penetration testing and security reviews, with reports (for example SOC2).
- To the extent not already covered above, implementing a policy for responding to cybersecurity incidents.
- Reviewing insurance coverage.

Allocation of risks and liabilities for cybersecurity

For business-to-business (B2B) arrangements in the technology sector, practitioners are increasingly seeing enhanced liability caps for customers covering breaches of information security, confidentiality and data protection terms.

Alternatively, some providers will offer a separate liability regime for defined losses flowing from cybersecurity breaches, such as the costs of notifying regulators and data subjects and offering identity-theft subscriptions for affected data subjects. Customers may also push for express terms stating that regulatory fines (where due to the provider's breach) are recoverable as direct losses or not subject to the liability caps.

Software providers will often seek to exclude all losses for loss or corruption of data, on the premise that:

- Where the customer is responsible for hosting, the customer is responsible for maintaining back-ups.
- Where the supplier is responsible for hosting, the supplier instead offers to restore the data according to its service level agreement (SLA) commitments.

For business-to-customer (B2C), it is generally more difficult to exclude or limit liability given the consumer rights and unfair terms protections.

Dispute resolution methods in relation to cybersecurity incidents

Practitioners have noted that claims following cyber and data security incidents are increasingly common. For information regarding disputes in the technology sector and cyber disputes in particular, see Sector note, Dispute resolution in the technology industry: Q&A.

UK and EU approaches to cybersecurity law and policy

EU-UK divergence or alignment

Prior to Brexit, the UK and EU were generally aligned on cybersecurity. In addition to sharing a legislative framework, public authorities and regulators shared information and closely cooperated on cybersecurity incidents likely to affect multiple member states. For example, under the NIS Directive, the ICO and NCSC liaised with their Member State counterparts, the European Commission, the European Network and Information Security Agency (ENISA), other EU and Member State regulators and the NIS Co-Operation Group.

Since Brexit, the global nature of cybersecurity has meant that similar concerns and policies apply in both jurisdictions. Unlike other areas, policymaking for cybersecurity has therefore continued along similar lines, although the mechanisms, timelines and details of requirements have started to diverge.

Examples relevant for organisations in the technology sector include:

- The EU Network and Information Security 2 Directive (EU) 2022/2555 (NIS 2 Directive) (applicable from 18 October 2024), will replace the NIS 1 Directive, and significantly widen and clarify the types of technology businesses within scope (see Practice note, NIS 2 Directive: overview). The UK, meanwhile, is still considering the outcome of its consultation on the changes to the UK NIS Regulations (the UK's existing implementation of the NIS 1 Directive), which may lead to similar (though less wide ranging) updates to the UK regime.
- The EU Digital Operational Resilience Act (DORA), and related DORA Directive (effective 17 January 2025) are designed to address the resilience of the EU's financial sector to ICT supply chain risks, including minimum contractual terms from ICT service providers, and subject critical ICT service providers to direct oversight by EU financial regulators. Financial entities will also be required to report major ICT-related incidents to their competent regulator (see Practice note, Hot topics: EU Regulation on digital operational resilience for the financial sector (DORA) and DORA Directive). Similarly, the UK financial regulators (BoE, PRA and FCA) have added to their existing outsourcing rules requirements for firms to map, test and address their operational resilience, as well as additional rules for outsourcing to critical third parties, see Practice note, Financial Services and Markets Act 2023: Critical third parties (CTPs) and Practice note, Hot topics: Operational resilience: UK regime for critical third parties to the financial sector.
- Although initially pursuing a 'soft' approach to regulation of the cybersecurity of connected devices through the Code of Practice for Consumer IoT Security, the UK has since enacted its consumer connectable product security regime (including the Product Security and Telecommunications Infrastructure Act 2022 (effective from 29 April

2024)). The EU, meanwhile, has proposed the EU Cyber Resilience Act to provide for minimum cybersecurity requirements for products with digital elements (see Legislation Tracker, Cyber Resilience Act: legislation tracker).

International-UK divergence or alignment

Prior to the UK general election in 2024, the UK Executive has generally pursued a 'lighter touch' approach to regulation which, in some cases, is at odds with the international direction of travel. For example, the UK has decided not to enact new legislation directed specifically at AI, unlike the EU and (with increasing likelihood) the US. It's unclear whether the same approach would continue under a different government party (if elected), or even if there were a significant change in personnel from the Executive at the date of this note.

Businesses operating in the technology sector should therefore keep an eye on the current (and coming) fluctuations in UK politics.

Sectoral trends

Future developments for cybersecurity in the sector

Regulators are likely to continue to issue cybersecurity-related rules and guidance specific to their sector, which will catch XTechs (where X is a particular vertical industry sector undergoing digital transformation such as AdTech, EdTech, FinTech, FoodTech, MedTech and RetailTech) subject to their authority.

At the UK's flagship cybersecurity conference, CYBERUK 2024, the Directors of the NCSC and GCHQ (the UK's intelligence, security and cyber agency) dedicated significant portions of their keynote speeches to the growing cyberspace threat of several States. State-sponsored cyber-attacks, and therefore cybersecurity, will continue to play an increasingly significant role in political disputes and global conflicts. As is demonstrated in the fall-out from the 2017 NotPetya attack (see Cybersecurity risks specific to the technology sector), this will present significant risks for technology organisations of all sizes and jurisdictions, their customers and other members of their custom and supply chains.

Cyber insurance is also likely to become increasingly expensive, with more extensive exclusions, for example for state-sponsored attacks.

A shortage in appropriately trained personnel is likely to impact on an organisation's ability to recruit and retain sufficient staff to tackle and implement its cybersecurity measures. Governments and organisations have already started to produce training and recruitment schemes, including those targeted at increasing diversity in the sector, and this trend is likely to continue to continue to grow.

Technical developments are, of course, also likely to impact an organisation's ability to keep on top of their cybersecurity measures. Increasing use of AI presents risks including evolving malware, data leakage through staff use of public versions of generative AI tools and growing reuse by tech providers of customer data, unanticipated inferences of information from datasets (public and private), and increasingly convincing phishing emails. Potential advances to quantum computing also present an as-yet near un-mitigatable risk for data security as current measures may be easily circumvented, such as de-crypting encrypted data, including any such information leaked or stolen now.