European cyber security law in 2023: A review of the advances in the Network and Information Security 2 Directive 2022/2555

Received (in revised form): 21st March, 2023

Charanjit Singh
Assistant Head, Principal Lecturer in Financial Law, Barrister-at-Law, University of Westminster, UK

Charanjit Singh PhD, is a Tenant and Barrister-at-Law at Holborn Chambers, and Assistant Head of School at the University of Westminster in London, UK. He has a PhD from the University of Southampton and writes extensively on corporate law, RegTech, artificial intelligence (AI) and evidence law. He has practised in professional and academic law for many years, with the aim of deconstructing the law for practitioners and academicians. His research explores the resultant effects of AI and the frameworks required to adequately regulate it.

Holborn Chambers, 6 Gate Street, London, WC2A 3HP, UK
E-mail: c.singh1@westminster.ac.uk

Abstract Cyber security capabilities must be designed to mitigate attacks and threats to key network and information systems and ensure continuity in service provision, contribute to the security and effective functioning of economies and societies, and the Network and Information Security 2 Directive (NIS2) seeks to strengthen the European Union (EU) approach to this. Advances in artificial intelligence (AI) have revolutionised industries including banking (FinTech), law (RegTech), insurance (InsureTech), charities (CharityTech) and health (HealthTech). The EU understands this and has therefore introduced the requirement for member states to embrace AI, as a cyber security tool used to protect against and prevent cyber security attacks/threats. The purpose of this paper is to review the NIS2 and the changes it makes to the European approach to cyber security including the use of AI, and the implications for businesses subject to the new rules. The subject is explored through an analysis of literature, EU law and policy documentation. This paper critically reviews a significant advent in European cyber security and technology law: the advances created by the NIS2 Directive, which are considered alongside other key legislation that came into force in January 2023. In addition, the UK's contrasting evolving position is also critically reviewed. The paper concludes with several practical suggestions on the, if any, steps for businesses as at April 2023. The NIS2 makes some significant inroads to close security gaps that existed in the EU cyber security-related legislative framework; importantly, it creates a requirement for the use of AI in the EU's cyber security defence armoury. Businesses need to undertake several steps in preparation for full implementation of the NIS2. This research is among the first to review key advances made in EU cyber security and technology law, and to contrast that with the UK position as at April 2023. It is also the first to discuss the likely powers of competent authorities, and the potential results of breaching other EU legislation such as the General Data Protection Regulation (GDPR).

KEYWORDS: cyber security, artificial intelligence, EU law, NIS2, cyberthreat, UK law

INTRODUCTION

Advances in technology, including artificial intelligence (AI), have fundamentally changed the way the world works. Technological sophistication of 'life' has resulted in a heightened risk in the opportunity for the commission of cybercrime.

AI has automated the tedious and time-consuming to generate cost and time efficiencies of significant scale; it has also actively innovated and improved 'the way things are done'.[1] AI and its constituent parts, ie machine learning (ML) and data analytics, have almost become colloquial terminology. These innovations have begun to be woven into every aspect of our lives, including economics, finance, environment, political, health, organisational, social and justice systems. The rationale is to provide innovative solutions to issues that academicians, governments and practitioners have tried to resolve.

These benefits are coupled with negative consequences where technology and AI are left insufficiently regulated and therefore vulnerable to exploitation. The European Union (EU) has recognised this, as has the UK and many other jurisdictions across the globe. Where the EU is concerned, there were significant deficiencies in the regulatory framework it designed to create a 'cybersecure' space where cyber threats/strikes were negated and a sufficient balance struck between the benefits of technological innovation and the detrimental potential of AI, ie the 'neutron-al' glue that bound the energies of AI to enhance innovation and provide stability to the present world and the future (the nucleus).

Several EU legislative acts seek to create a cohesive framework ('the glue') and 'build trust' in AI through the creation of a 'safe and innovation friendly environment'[2] for all stakeholders including consumers, creators and businesses. This paper critically reviews the advances in cyber security brought in by the Network and Information Security 2 (NIS2) and explores its practical implication on pan-European businesses.

EUROPEAN CYBER SECURITY

Significant vents in European cyber security

The EU began its AI engagement journey circa 2018 with a proposal for the creation of an AI Expert Group and European AI Alliance.[3] It is evident that this change of heart came in response to Japanese, American, Canadian and Chinese AI strategies.[4] The primary focus of the EU was on an ethical development of AI that was grounded in its fundamental principles, rights and values, including the protection of data, safety and security, innovation, transparency and fairness, open democracy. The former President of the European Commission (EC), Jean-Claude Juncker, in his 2017 State of the Union address, opined that 'Europe is still not well equipped when it comes to cyber-attacks. [Therefore], today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks.'[5]

The EU acknowledged that the manifest opportunities created by AI also came with several new and novel risks including fraud, the theft of data, misinformation and destabilisation of economies and governments. In 2016, 4000+ daily ransomware attacks occurred, and at least 80 per cent of EU economies were the subjects of a cyber security 'incident'. There was a 500 per cent increase in cybercrime in the period 2013–17. Thus, measures to integrate strong levels of cyber security in the EU were proposed by the EC and the High Representative. They included:[6]

- Create a robust EU Cybersecurity Agency built on ENISA (the Agency for Network and Information Security) to deal with cyberattacks/strikes on EU member states;
- Create an EU Cybersecurity Certification Scheme for digital products and services;

- Create a criminal law-based response to cybercrime;
- Create a Directive to combat fraud-related financial crime and the counterfeiting of non-cash payments systems/means;
- Have in place blueprints for continuity in the event of large-scale cyberattacks/strikes;
- Have pan-European Cybersecurity Research and Competence Centres focused on assisting in updating the tools and technology that are needed to counter cyberattacks/strikes;
- Provide a training and education platform on cyber defence;
- Strengthen international cooperation on cyber security between the EU and North Atlantic Treaty Organization (NATO) via joint diplomatic responses to malicious cyber activity.

Sectoral trends: The need for EU cyber security measures

During July 2021 to June 2022 sector-targeted incidents of cyberattacks/strikes in the EU were as follows: 13.09 per cent — digital service providers, 8.64 per cent — finance and banking, 24.21 per cent — government/public administration, 7.2 per cent — health; 8.12 per cent — transport and energy.[7] There are three motivations: monetisation — these are finance-related actions undertaken by cybercriminals/gangs; geopolitical — espionage and disruption, often state-sponsored; and ideological, also referred to as 'hacktivism', ie action seeking to *further a cause* or ideology.

Thus, finance and banking is the sector most often targeted by cybercriminals and experiences a significant number of cyberattacks/strikes because it is the most lucrative for criminals; access to it can result in significant profit via extortion, fraud and theft.[8] Cybercriminals often look for vulnerabilities and organisations with manual systems are particularly vulnerable; this allows cybercriminals to steal identities, launder money, finance terror, steal intellectual property, counterfeit currency, abuse credit cards and carry out computer-related fraud and theft. Therefore, advances in cybercrime, criminal law and civil law systems (compensation) seek to provide a framework by which criminals can be brought to justice (prosecuted) and victims can be compensated, and cyber security provides the framework to try and prevent businesses, consumers, and governments from being vulnerable to exploitation. What follows is a review of the NIS2.

NIS2 Directive 2022/2555

The global cost of cybercrime in 2020, as estimated by the EC, stands at €5.5tr.[9] The NIS Directive was the first piece of pan-EU legislation focused on cyber security; its implementation across the EU member states was troublesome and adoption was patchy. The NIS applies to essential and important entities operating within a defined list of sectors, ie ones that relate to 'critical infrastructure'. The NIS2 replaces the NIS as proposed by the EC. The NIS2 advances minimum requirements in cyber security measures designed to deal with specific risks (discussed later).

In November 2022, the European Parliament amended EU Law so that investment in critical cyber security infrastructure and pan-EU rules could be further strengthened. Key advances in the NIS2 Directive include:

- Broadening application to greater number of entities/sectors than covered by the NIS;
- Member states can prescribe the use of information and communications technology (ICT) processes, products and services certified under the Cyber Security Act;[10]
- Greater level of accountability and direct obligations on 'management bodies' in relation to implementation and supervision of legislative compliance. Penalties for failures include fines and

temporary disbarment from discharging managerial/senior managerial functions;
- Requirement to implement cyber security risk mitigation and due diligence in terms of third-party service providers and/or suppliers;
- Promotion of information system development practices including cryptography, encryption, multi-factor authentication and disclosure of vulnerabilities;
- Additional phased notification obligations: (a) initial (24-hours) in contrast to the NIS required notification 'without undue delay'; (b) intermediate; and (c) final reporting obligations;
- Implementing policies on business continuity, handling of incidents, information security, analysis of risk and security in the supply chain;
- Member states have the discretion to set dissuasive, effective and proportionate penalties for breach, in addition to administrative fines to a maximum of €10m or 2 per cent of global turnover.

The NIS2 Directive (2022/2555) came into force on the 16th January, 2023 and must be transposed by 18th October, 2024 into member state legal systems by legislative acts (standard procedure for Directives).[11] The UK government has confirmed that it will also be updating the NIS regulations as they apply to the UK.[12] Therefore, the cyber security landscape in both the EU and UK[13] will remain both complex and challenging.

The NIS2: Effect

There are several advances that the NIS2 seeks to make to the security gaps under the original NIS regime. What follows is a discussion of some of the most salient changes.

Scope: Expansion

The original NIS can be attributed the glory of being the first pan-EU cyber security law. It came into force in 2016 and its purpose was to harmonise cyber security in the EU. Therefore, operators of 'essential services' were required to implement *risk management* and were subject to *reporting obligations*; these included health and energy entities, infrastructure businesses and transport, and those offering digital services, ie cloud computing and search engine facilities, etc.

The new law, as set out in the NIS2,[14] advances on 'essential' entities by also adding those considered to be 'important', and it has a sectoral application which is far broader than its predecessor. The result is that organisations that did not previously fall under the ambit of the NIS are likely to fall within the remit of the NIS2. Annex I ('essential') and Annex II ('important') of the NIS2[15] set out the full lists. These can be summarised as:

Important
- Couriers;
- Chemical distribution and waste management;
- Digital providers (online marketplaces, search engines, social networking sites, data centres);
- Food distribution, production and processing;
- Manufacturing of electrical products, medical devices and transport;
- Postal services and research.

Essential
- Banking;
- Energy and drinking water;
- Digital services/infrastructure and financial markets infrastructure;
- Health and public services (excluding the judiciary, Parliament and central banks);
- Transport and space.

The reach of the NIS2 will only be known when it is fully implemented. Further detail is also provided within the NIS2 on which entities within the sectors identified are subject to the law. Member states have been

tasked with creating the list of those entities that are subject to the NIS. The NIS2 creates a size cap on relevant medium and large entities that are required to comply with it. It is worth noting that the NIS2 applies to all those entities that are considered *essential* and *important* irrespective of their size where they provide public electronic communications networks and/or services, where potential disruption of a service offered could impact on public safety, health and security, or where potential service disruption could cause systemic risk, especially in sectors concerning cross-border activity that could result in a ripple effect. Additionally, an entity can be designated as being essential or important where the size threshold is not met if it is the sole provider of a service critical to economic or social activity. All EU member states have until 17th April, 2025[16] to determine a list of essential and important entities subject to the NIS2.

Cyber security risk management: Key measures

The NIS2 has streamlined the cyber security management approach to reduce resilience inconsistencies across all relevant sectors. With this endeavour in mind, it introduces key measures that all entities falling within the remit of the NIS2 must undertake to manage cyber security risks relating to their networks and information systems. They include:

- Business continuity management;
- Crisis management;
- Cryptography;
- Encryption;
- Frameworks and processes to assess the effectiveness of adopted cyber security risk management measures;
- Handling of incidents: detection, prevention and response;
- Network and information system security: acquisition, disclosure, development and maintenance and handling of vulnerabilities;
- Risk analysis;
- Security of information systems;
- Security in the supply chain: data storage, key relationships with suppliers, etc.

Cyber security risk management: Liability and corporate accountability

Under the new regime, the NIS2 has increased the responsibility that 'management bodies' (MB) bear in assuring compliance with the law.[17] Therefore, on implantation of the Directive the member state must ensure that its MBs do the following:

- Approve all relevant cyber security risk management measures to be undertaken by the entity in ensuring compliance with the directive for example security in the supply chain;
- Undertake regular (specific) training in the knowledge and skills to be able to apprehend, assess, manage and oversee the cyber security risks posed to their essential or important entity;
- Supervise the implementation of relevant risk management measures;
- Entities hold MBs to account in the event of non-compliance.

The result of this is to render the MB of an entity liable on a breach of the NIS2. This elevates the responsibility of managing cyber security risk to an entity's senior management. Therefore, the MB has ultimate responsibility, and a dereliction of duty could well result in the entity's management being liable for both breach and fines, as set out in the legislation passed by the respective member states on adoption of the NIS2 into their legal systems.

The Directive also gives the member state the discretion to define what it considers to be the MB, the terminology is not defined in the NIS2, other than the suggestion that individual(s) that discharge managerial functions could well constitute a MB for the purposes of the Directive. Therefore, the

MB is most likely to include the board of directors and various company executives. It would be these individual(s) who would also be the subject of enforcement actions taken for an entity's failure(s) to comply with the law. When transposing the NIS2 member state legislation can ban individuals at a senior level (C-suite) from continuing to discharge managerial functions until such time that identified deficiencies are remedied and/or compliance with requirements of the competent member state authority (as designated) is achieved.

Like the powers of other industry regulators, under the NIS2 a member state can request that an entity in breach make a public statement regarding the occurrence of an infringement[18] and name those that are responsible for it. This is designed to pose 'reputational risk' and act as a deterrence. Experience informs us that this latter factor, like that in the regulation of financial services, can often be successfully mitigated by well-funded communication management teams.

Member states are also given the scope to set appropriate penalties, but these must be dissuasive, effective and proportionate.[19] The NIS2 (Recitals) make it clear that penalties include punishment under the criminal law. Therefore, compliance teams and lawyers' departments, whether internal or external to the entity, must be aware of any civil and/or criminal penalties that are provided for by the legislation that transposes the NIS2 into their domestic law.

Reporting requirements: A 3-tier approach

In contrast to its predecessor, the NIS2 provides specific provisions on reporting, report content and timeframes. Essential and important entities are required to notify the member state's 'competent authority' or a 'Computer Security Incident Response Team'[20] of any incident(s) of *significant impact on the services they are providing or the recipients of those services*. Notably, this includes any incident(s) that can potentially cause or have caused disruption to the entity's operations or substantial financial loss and cyber security threats/strikes that could have resulted in the occurrence of a significant incident.

The NIS2 has introduced the following 3-tiered approach:[21]

- *First tier*: Early warning, on becoming aware of the incident notify within 24 hours. Change: from reporting 'without undue delay' (NIS), to initial notification (NIS2);
- *Second tier*: Intermediate notification, notify within 72 hours of becoming aware of an incident. Provide an initial assessment of incident impact and severity, and any indicators of compromise;
- *Third tier*: Final report, submit within one month of the incident notification, must include a detailed report of incident and cause.

Incidents reported under the NIS2 involving personal data are likely to breach the EU General Data Protection Regulation 2016/679 (GDPR) and therefore, the Directive states that the 'competent authority' is required to inform the relevant 'data protection authority' of incident(s) that amount to notifiable breaches of personal data.[22] To avoid double penalisation where a fine is imposed by the data protection authority for a GDPR violation, the NIS2 competent authority cannot then impose a financial penalty for the same incident. The NIS2 competent authority can, however, impose any non-financial penalties that it has at its disposal, ie adhering to deadlines for rectifications resulting from a cyber security audit or publish details about the infringement.

Competent authority enforcement powers

The NIS2 clarifies which competent authority is tasked with supervision.

Essential and important entities are subject to supervision from the competent authority of the member state in which it is established. If it is a cloud computing digital infrastructure provider, then jurisdiction lies with the competent authority of the member state that is its 'main EU establishment' (ME).[23] The ME is the location in which the entity makes decisions relating to its cyber security risk management measures; if that cannot be determined and/or if these decisions are taken outside of the EU, then the ME is the location within the EU in which the entity's cyber security operations are undertaken. Where this proves problematic in determining the ME, then it is the member state in which the entity has the most EU employees.[24]

Entities that are established outside of the EU must designate an EU representative in any EU member state where they offer their services. The regime of supervision and enforcement penalties[25] that have been afforded to national (competent) authorities per the NIS2 are more detailed than those in the NIS. Thus, the competent authority may:

- Carry out on-site security audits and inspections;
- Make requests for information to help it assess an entity's cyber security measures;
- Carry out a security scan;
- Make requests for access to information that facilitate the assessment of cyber security risk-management measures, allowing it to determine the level of implementation of data and policies.

The NIS2 allows a competent authority to investigate *essential entities* at any time, whether regularised or random. In contrast, important entities can only be investigated ex-post (after an incident has occurred). In terms of breaches of cyber security risk management measures or incident reporting obligations, the NIS2 allows the implementation of administrative fines for *essential entities* at a minimum of €10m (as stated earlier), or 2 per cent of global turnover for the previous financial year — the greater of the two figures wins. For important entities it is €7m or 1.4 per cent of global turnover, again the greater of the two figures.[26] The competent authority can also impose non-financial penalties such as orders to comply, implement cyber security audit findings, to inform stakeholders and to make public information.

The NIS 2 and AI

The NIS2 Directive requires EU member states to promote innovative technologies including AI[27] so that cyberattack detection and prevention can be greatly improved. The rationale is that this could facilitate a more efficient allocation of finite financial resource so that such criminality can be successfully combatted. Paragraph 51 specifically states that:

> 'Member States should therefore *encourage in their national cybersecurity strategy activities in research and development to facilitate the use of such technologies, in particular those relating to automated or semi-automated tools in cybersecurity*, and, where relevant, the sharing of data needed for training users of such technology and for improving it. The use of any innovative technology, including artificial intelligence, should comply with Union data protection law, including the data protection principles of data accuracy, data minimisation, fairness and transparency, and data security, such as state-of-the-art encryption. The requirements of data protection by design and by default laid down in Regulation (EU) 2016/679 should be fully exploited.'

In addition, Paragraph 89 states that:

> 'Essential and important entities should … evaluate their own cybersecurity capabilities and, *where appropriate*, *pursue*

the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems.'

The NIS2 promotes AI in supporting cyber security endeavours at both a state and entity level. In terms of the former, the member state is encouraged in its 'national cybersecurity strategy activities in research and development to facilitate the use of [AI]', and the latter, 'where appropriate, pursue the integration of cybersecurity enhancing technologies [such as AI]'. This is very much the promotion of the use of AI as a tool to enhance cyber security throughout the EU. Many entities, important and essential, already adopt AI as part of their armoury against cyberattacks, therefore this may be more meaningful at a member state level.

Evidence on the innovation in AI shows that the cybercriminals are finding new and novel ways in which to outsmart the technology and exploit vulnerabilities. Complexities in entity network infrastructure mean there are more opportunities to access it for purposes of exploitation, and thus the cyberthreat is growing exponentially, but equally the technology is developing at an astounding rate to counteract this.[28] The frameworks to regulate the innovation of AI are slow to catch up with advents in the field. From a cyber security perspective, the EU clearly understands how AI can assist entities — for example, in the analysis and monitoring of large amounts of unstructured complex data, minimising false alarms and avoiding human error while saving cost and time. It also understands that this may mean that actual attacks/threats can be more readily detected and/or prevented. But the NIS2 leaves questions relating to bias and discrimination, transparency and accountability to 'other' legislation.

That said, the NIS2 cannot be viewed in a vacuum. It is complemented by a raft of new EU measures aimed at this area, including the Digital Operations Resilience Act (DORA), the Critical Entitles Resilience (CER) and the Artificial Intelligence Act. The latter seeks to harmonise rules on AI and regulating AI systems operators[29] across the EU through the following:

- Reduce risk attached to operating AI systems;
- Harmonise the rules on market placing, delivery for use and use of AI systems;
- Introduce a risk-based approach to AI: the greater the risk an AI system poses, the more stringent the regulatory requirements;
- Introduce specific requirements for high-risk AI systems and compliance obligations for the operators;
- Introduce transparency requirements for AI systems that interact with the public, detect emotion, categorise biometrics and for those that manipulate content, visual images, sounds and video;
- Create a list of prohibited practices;
- Introduce fines for breach of the AIA of up to €500,000.

DORA — Regulation (EU) 2022/2554

DORA comes into force in 2025. Approved on 22nd November, 2022 at the European Parliament's plenary session, it seeks to harmonise and improve operational resilience in European financial services. Its focus is to ensure that the EU's financial sector is resilient to cyberattacks/strikes and operational disruptions. Therefore, banks, crypto-asset service providers, electronic money providers, investment companies, payment providers and third-party ICT providers will all be subject to these new rules. Furthermore, supervision, enforcement and implementation is delegated to national authorities. Greater discussion on DORA is beyond the scope of this paper.

CER — Directive 2022/2557

The CER Directive 2022/2557 replaces the European Critical Infrastructure Directive 2008/114/EC. This came into force in January 2023.[30] The CER complements the NIS2 and reinforces the resilience of European critical infrastructure against natural hazards, insider threats, sabotage and terror attacks. It applies to the following 11 sectors: banking, digital infrastructures, drinking water, energy, financial market infrastructures, food, health, public administration, space, transport and wastewater. The CER requires all member states to undertake risk assessments on a regular basis with the purpose of identifying entities critical or vital to the economy and functioning of civil society. Greater discussion on the CER is beyond the scope of this paper.

CONTRASTING THE EU AND UK APPROACH

The respective regimes in the UK and EU are aligned since the UK's withdrawal from the EU. The anecdotal evidence suggest that 'some' divergence will take place in relation to the UK's approach to the regulation of critical cyber security infrastructure, but this is unlikely to be significant. Thus, the UK regime will almost certainly align itself with the NIS2 in relation to managed services, incident reporting, outsourcing, security of the supply chain and in terms of business continuity, and this is sensible. The UK government has confirmed that it will refresh the UK NIS Regulations, and some of the proposed changes are similar to, if not the same as, those set out in the NIS2.[31] The key difference relates to the timeframe in which the UK will make these changes; this requires an Act of Parliament which can be a lengthy process, and thus, a timeline for refreshing the regulations has not been set.

Like the EU, in the UK, digital 'managed' service providers (DMSP) are being brought within the regulatory gaze; therefore, DMSPs will be subject to the same rules and obligations as digital service providers currently subject to the existing regulations. The UK, like the EU, may also choose to bring 'other' critical sectors into the scope of its regulations with greater ease. The financial sector in the UK is not currently subject to the NIS but is facing greater regulatory requirements from the incoming PS2/21 (Solvency II)[32] and Financial Services and Markets Bill,[33] which seek to manage deterioration of service, supplier failure and concentration risk.

Currently, UK entities that are regulated by the NIS will need to carry on implementing cyber security measures that the sectorial competent authorities require them to. The UK government has indicated its preference for a toolkit approach to promote greater flexibility akin to the Cyber Assessment Framework.[34]

At present, data breaches and security incidents must be notified to the relevant authorities. Both the EU and the UK are seeking to encourage greater levels of reporting. The UK is updating reporting requirements and the definition of 'incident' will be expanded to include those that 'do not actually affect the continuity of the service directly, but nonetheless pose a significant risk to the security and resilience of the entities in question and the essential services they provide'.[35] The UK text and sectorial thresholds are yet to be determined, but it is likely to retain the 72-hour reporting deadline which will contrast with the EU's three-tiered approach.

Additionally, the UK is likely to require its 'essential' and 'important' entities to adopt similar technical and organisational measures for the management of cyber security threats and risks to systems and operations, but this is not fully set out and could very well change. In terms of jurisdiction, the likelihood is that the UK will adopt a framework like that in the NIS2 for organisations that provide services in the UK while being physically located

outside of it. This proposal is yet to be fully determined.

Finally, in terms of compliance, the framework within the UK provides for fines of up to £17m but, unlike the EU, does not give an option for this to be equivalent to 2 per cent of total worldwide turnover, etc. Thus, it is far more limited in scope.

CONCLUSION AND PRACTICAL STEPS

The NIS2 came into force in January 2023; member states must implement it by the 18th October, 2024. Therefore businesses located within the EU or those falling with the definition of ME (as above) need to consider the following:

- Determine whether the services or activities they provide fall within the ambit of the NIS2 regime, and if the answer is in the affirmative, identify the companies or subsidiaries affected;
- Start to assess security controls and protocols in place and revise relevant polices/processes;
- Start to prepare or amend plans and policies from a financial, organisational and technical perspective to assure compliance;
- Plan relevant documented processes in preparedness for due diligence;
- Ensure that changes, controls and incident response measure obligations are properly communicated with suppliers so that supply chain risk and reporting requirements are adequately addressed;
- Create or revise an ICT plan: the EC predicts that the NIS2 will create additional spend of at least 20–22 per cent for entities that are not subject to the NIS but fall within the remit of the NIS2, and a minimum 10–12 per cent for those already in the current NIS regime.

UK organisations should review the NIS2 and its impact as it is likely that the regulatory regime will be similar, even though it is evolving. The UK regime is unlikely to see parliamentary time before the next general election and therefore is unlikely to be updated until 2024/25.

Given the automation and digitalisation of many functions, organisations would be prudent, at the very least, to begin to engage with AI and the benefits of this technology as part of the armoury to guard against cyberthreats/strikes and for enhanced cyber security.

References

1. In relation to efficiencies see, Singh, C. and Lin, W. (2020), 'Can Artificial Intelligence, RegTech and CharityTech provide Effective Solutions for Anti-money Laundering and Counter-terror Financing Initiatives in Charitable Fundraising', *Journal of Money Laundering Control*, Vol. 24, No. 3, pp. 464–482.
2. Artificial Intelligence for Europe, 'COM (2018) 237 Final'. See also, 'Digitising European Industry Reaping the full benefits of a Digital Single Market, COM (2016) 180 Final and Investing in a smart, innovative, and sustainable Industry A renewed EU Industrial Policy Strategy, COM (2017) 479 Final'.
3. European Commission (March 2018), 'Artificial intelligence: Commission kicks off work on marrying cutting-edge technology and ethical standards', Press Release, Brussels.
4. European Commission, European Political Strategy Centre (2018), 'Strategic Note: The Age of Artificial Intelligence'; European Commission, European Political Strategy Centre (2019), 'The age of artificial intelligence: Towards a European strategy for human-centric machines', Publications Office; McKinsey Global Institute (February 2019), 'Notes from the AI Frontier, tackling Europe's Gap in Digital and AI', available at https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/tackling%20europes%20gap%20in%20digital%20and%20ai/mgi-tackling-europes-gap-in-digital-and-ai-feb-2019-vf.pdf — the announcement of €1.7bn AI technology park in Beijing. See also Larson, C. (February 2018), 'China's massive investment in artificial intelligence has an insidious downside', Science, available at https://www.science.org/content/article/china-s-massive-investment-artificial-intelligence-has-insidious-downside (both accessed 21st March, 2023).
5. European Commission (September 2017), 'State of the Union 2017 – Cybersecurity: Commission scales up EU's response to cyber-attacks', Brussels, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193 (accessed 21st March, 2023).
6. European Commission, ref. 4 above.
7. European Union Agency for Cybersecurity (ENISA) (October 2022), 'Threat Landscape 2022', available

at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (accessed 21st March, 2023).
8. Note that these factors would not normally be the motivation for state-sponsored cyberattacks or for hacktivists.
9. European Commission (January 2021), 'A cybersecure digital transformation in a complex threat environment', Brussels.
10. Regulation (EU) 2019/881 of the European Parliament and the Council of Europe of 17 April 2019, on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), paras. 69–70. The Cybersecurity Act strengthens the EU Agency for Cybersecurity (ENISA) and creates the Cybersecurity Certification Framework for Products and Services.
11. For a detailed discussion in relation to EU Law and implementation see Lenaerts, K., Van Nuffel, P. and Bray, R. (2011), *European Union Law*, Sweet and Maxwell, London.
12. Department for Digital, Culture, Media & Sport (November 2022), 'Government response to the call for views on proposals to improve the UK's cyber resilience. Consultation Outcome', Gov.UK, available at https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/outcome/government-response-to-the-call-for-views-on-proposals-to-improve-the-uks-cyber-resilience#:~:text=The%20proposals%20regarding%20digital%20service,for%20improvement%20were%20also%20noted (accessed 21st March, 2023).
13. In terms of the UK see, the Cyber Resilience Act, the Critical Entities Resilience Directive, the Digital Operational Resilience Act (DORA) which focuses on financial services and the reforms to the UK's Network and Information Systems Regulations.
14. European Union Agency for Cybersecurity (ENISA) (2023), 'Supporting the implementation of Union policy and law regarding cybersecurity', available at https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new (accessed 21st March, 2023).
15. Article 3, Annex I and II. Directive (EU) 2022/2555 of the European Parliament and The Council, available at https://eur-lex.europa.eu/legal-content/En/TXT/HTML/?uri=CELEX:32022L2555&from=EN.(accessed 21st March, 2023).
16. Article 3(3), Directive (EU) 2022/2555.
17. Article 20 and 21, Directive (EU) 2022/2555.
18. Articles 23 and 32, Directive (EU) 2022/2555.
19. Article 36, Directive (EU) 2022/2555.
20. Article 23(1), Directive (EU) 2022/2555. See also, Articles 1 and 10, Directive (EU) 2022/2555.
21. Article 23(4), Directive (EU) 2022/2555.
22. Article 35, specifically paragraph 3, Directive (EU) 2022/2555.
23. Article 26, Directive (EU) 2022/2555.
24. Article 2(2), Directive (EU) 2022/2555.
25. Articles 32–36, Directive (EU) 2022/2555.
26. Article 34, specifically paragraphs (4) and (5), Directive (EU) 2022/2555.
27. Paragraphs 51 and 89, Directive (EU) 2022/2555.
28. Singh and Lin, ref. 1 above.
29. This also includes suppliers who market or deliver such systems for use in the EU, systems users that use AI to in professional and/or gainful activity. Note, the AI Civil Liability Directive is also likely to be finalised by March 2023, this creates non-contractual claims for damages based on tortious liability.
30. For a general discussion see, Pursiainen, C. and Kytömaa, E. (2023), 'From European critical infrastructure protection to the resilience of European critical entities: What does it mean?', *Sustainable and Resilient Infrastructure*, Vol. 8, No. 1, pp. 85–101.
31. Department for Digital, Culture, Media & Sport (November 2022), 'Proposal for Legislation to Improve the UK's Cyber Resilience, Consultation outcome', Gov.Uk, available at https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience (accessed 21st March, 2023).
32. The PRA policy statement (PS2/21) sets out the expectations and guidance relating to the work of auditors on matching adjustment (MA) under the Solvency II regime.
33. HM Treasury (November 2021), 'Future Regulatory Framework Review: Proposals for Reform', Gov.UK, available at https://www.gov.uk/government/consultations/future-regulatory-framework-frf-review-proposals-for-reform (accessed 21st March, 2023).
34. The Cyber Assessment Framework provides a systematic approach to the assessment of how well cyber risks relating to essential functions are managed by an entity. The framework can be used by an entity itself or a third-party for example a competent authority, or a professional service provider acting on its behalf.
35. Department for Digital, Culture, Media & Sport, ref. 12 above, para. 5.4.