The European Approach to Cybersecurity in 2023: A Review of the Changes Brought in By the Network and Information Security 2 (NIS2) Directive 2022/2555

Singh, C.

The European Approach to Cybersecurity in 2023: A Review of the Changes Brought in By the Network and Information Security 2 (NIS2) Directive 2022/2555.

Singh, C.*

Key Terms: Cybersecurity, European Law, NIS2, UK Law, Cyberthreat, Artificial Intelligence.

Abstract

Purpose: Artificial intelligence (AI) is revolutionising Banking (FinTech) and Law (RegTech), as well as many other sectors including Charities (CharityTech) and Health (HealthTech). AI is continuing to push the parameters in which it has integrated itself into critical functions, economically and socially. Innovating and embracing the benefit of AI also means having a robust protection system to prevent cybersecurity breaches and/or strikes that seek to damage, destroy, or unlawfully profiteer from those benefits. The purpose of this article is to review the NIS2 and the changes it makes to the European approach to cybersecurity, and the implications for businesses subject to the new rules.

Design/methodology/approach: This subject is approached through the analysis of literature, European law, and policy documentation. The article presents with a review of the changes to the current European approach brought in by the NIS2 alongside some other key EU legislation that also came into force in January 2023, a contrast with the UKs evolving position, and concludes with practical suggestions on next steps for businesses as at February 2023.

Findings: Several steps are suggested for business to undertake in preparing for full implementation of the NIS2.

Originality: The work is original because it one of the first to review the changes made by key EU legislation in relation to the European approach to cybersecurity and provides contrast with the UKs position as at February 2023, discuss the likely powers of the competent authority and aspects such what happens in the event other EU law is also breached, for example the GDPR.

Introduction

Artificial intelligence (AI) is changing the way in which the world works. The ability of AI to automate the 'tedious' and 'time consuming' generates time and cost efficiencies but it is also actively innovating and improving 'the way things are done'[1]. AI, machine learning (ML) and data analytics have become commonplace, perhaps even colloquial. This innovation has great potential and must be woven into the fabric of economic, environmental, financial, health, organisational, political, and social and justice systems to provide innovative solutions to issues academics, governments and practitioners have long grappled with.

Factors such as these, amongst others, can be classed as potential benefits, but there is dark side to AI when left inadequately protected. There were distinct deficiencies in the regulatory frameworks to create a 'cybersecure' space in which cyber-attacks/strikes are negated and a balance struck against the detrimental potential of AI i.e., a 'neutron-al' glue that binds the energies of AI to enhance innovation and provide stability to the world in which we exist now and, in the future, (the nucleus). The European approach seeks to establish this 'glue' and 'build trust' in AI by creating a 'safe and innovation friendly environment'[2] for all stakeholders, whether they are consumers, creators, or businesses through various supporting cybersecurity measures. This article reviews the changes in the European approach to cybersecurity brought in by the Network and Information Security 2 (NIS2) and sets out the practical implication of this new law, if any, on pan-European businesses.

1. European Approach

1.1. Significant Advents in EU Cybersecurity

The European Union (EU) 'milestones' on greater engagement with AI began in earnest circa 2018 with the proposed creation of an 'AI Expert Group' and a 'European AI Alliance'[3]. It is fair to state that this response came in the wake of American, Japanese, Chinese and Canadian strategies relating to AI[4]. The EU's focus from the outset was on ethical AI development grounded firmly in the Union's fundamental principles and rights including data protection, fairness, transparency, innovation, safety and security, and democracy. In 2017, former European Commission (EC) President, Jean-Claude Juncker in his State of the Union address opined "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

[1] In relation to efficiencies see: Singh, C., et al. (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] Artificial intelligence: Commission kicks off work on marrying cutting-edge technology and ethical standards. European Commission Press Release. Brussels, 9 March 2018.

[4] European Commission, European Political Strategy Centre. Strategic Note: The Age of Artificial Intelligence, 2018. European Commission, European Political Strategy Centre. The age of artificial intelligence: towards a European strategy for human-centric machines, Publications Office, 2019, https://data.europa.eu/doi/10.2872/23955. And the McKinsey Global Institute. Notes from the AI Frontier, tackling Europe's Gap in Digital and AI. February 2019 – the announcement of 1.7€ billion AI technology park in Beijing. See also: Larson, C. China's massive investment in artificial intelligence has an insidious downside. Science, February 8, 2018.

defend us against such attacks"[5]. Thus, the EU acknowledged that whilst AI can lead to opportunities it has created new and novel risks relating to data theft, fraud and the destabilisation of economies and governments. In 2016, there were over 4000 ransomware attacks per day, and 80% of EU economies were subjected to at least one cybersecurity 'incident'. Thus, cybercrime between 2013 – 2017 rose by 500%. Therefore, the EC and the High Representative proposed measures to integrate strong levels of cybersecurity in the EU, this included[6]:

- The creation of a stronger EU Cybersecurity Agency built on ENISA (the Agency for Network and Information Security) to deal with cyber-attacks on EU member states.
- Creation of a pan-EU cybersecurity certification scheme for digital products and services.
- Blueprints for continuity in the event of largescale cyber-attacks/strikes.
- Pan-European Cybersecurity Research and Competence Centres to assist in updating the tools and technology needed to counter cyber-attacks/strikes.
- The creation of a Directive to combat financial crime related to fraud and the counterfeiting of non-cash payments systems/means.
- Create a more efficient response to cybercrime grounded in criminal law.
- Strengthen international cooperation on cybersecurity between the EU and NATO via joint diplomatic responses to malicious cyber activity.
- Provision of a cyber defence training and education platform.

1.2. Sectoral Trends and the Need for EU Cybersecurity Measures

In the period July 2021 – June 2022, pan-EU sector-targeted incidents[7] of cyberattack/strike were as follows: health – 7.2%, 8.64% – finance and banking, 24.21% – government/public administration, 13.09% – digital service providers, and 8.12% – transport and energy. The main motivation of these are as follows:

- Monetisation, a finance related action undertaken by cybercriminals and/or groups.
- Geopolitics: espionage and disruption, usually state sponsored.
- Ideological, 'hacktivism' – action that seeks to *further a cause* or ideology.

Thus, these sectors are leading targets for cyber-criminals and cyber-attacks/strikes; finance and banking are where the money is, and access often facilitates profit via extortion, fraud, and theft[8]. It is salient to note that cybercriminals seek to exploit vulnerabilities to benefit from identity theft, theft of intellectual property, money laundering, terror finance, credit card abuse, counterfeiting currency, computer related fraud and theft. Thus, advents in cybercrime, or criminal law, seek to provide the framework in which criminals can be prosecuted, cybersecurity is the framework that seeks to prevent business, consumers, and governments from being vulnerable to exploitation. What follows is a review of some of the measures enacted by the EU to protect its member states, business and consumers.

Network and Information Security (NIS2) – Directive 2022/2555

[5] State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks. European Commission Press release. Brussels, 19 September 2017.
[6] Ibid, note 4.
[7] European Union Agency for Cybersecurity. ENISA Threat Landscape 2022. ENISA, October 2022.
[8] Note that these factors would not normally be the motivation for state-sponsored cyber-attacks or for hacktivists.

The EC estimated that the global cost of cybercrime in 2020 at €5.5 trillion[9]. The Network and Information Security (NIS) Directive was the first pan-EU legislation focussed on cybersecurity, the implementation of which was troublesome; the result was patchy adoption across EU member states. The NIS applied to essential and important entities operating within a defined list of sectors i.e., ones that relate to 'critical infrastructure'. The EC proposed that the NIS be replaced by the NIS2. The NIS2 introduces a minimum requirement of cybersecurity measures designed to deal with specific risks (discussed below). In November 2022, the European Parliament (EP) amended EU Law so that further investment in critical cybersecurity infrastructure and pan-EU rules could be strengthened. Key developments in the NIS2 Directive include:

- Application to a broader range of entities/sectors than those covered by NIS.
- The ability of member states to prescribe the use of particular ICT processes, products and services as certified under the auspices of the Cyber Security Act[10].
- Imposition of greater accountability and direct obligations on 'management bodies' with respect of implementation and supervision of legislative compliance, penalties for failures include fines and temporary disbarment from discharging managerial/senior managerial functions.
- Implementation of cybersecurity risk mitigation and due diligence in relation to third-party service providers and/or suppliers.
- Information system development practices including cryptography, encryption, multi-factor authentication and disclosure of vulnerabilities.
- Additional phased notification obligations: initial (24-hours) unlike the NIS which provided for notification 'without undue delay', and intermediate and final reporting obligations.
- Implementation of policies on continuity of business, incident handling, information security, risk analysis and security in the supply chain.
- Gives member states discretion to set dissuasive, effective, and proportionate penalties for breach, in addition to administrative fines the tune of up to 10M€ or 2% of global turnover.

The NIS2, or Directive 2022/2555, entered into force on the 16.01.2023. This new pan-EU cyber-law must be implemented (transposed) by member states by 18.10.2024 into their legal systems by legislative act (standard procedure for Directives)[11]. The UK has also confirmed that it will be updating the NIS regulations as they apply to the UK[12]. Thus, the cybersecurity landscape across the EU and the UK[13] is likely to remain complex and challenging.

[9] European Commission. A cybersecure digital transformation in a complex threat environment. Brochure. Brussels, 28 January 2021.

[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). See 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. UK: Sweet and Maxwell.

[12] Government response to the call for views on proposals to improve the UK's cyber resilience. Consultation Outcome, 30 November 2022. UK: HMSO.

[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.

Critical Entities Resilience (CER) – Directive 2022/2557

Whilst a greater discussion is beyond the scope of this article, it is salient to note that the Critical Entities Resilience (CER) Directive 2022/2557, which replaces the European Critical Infrastructure Directive 2008/114/EC also came in force in January 2023. The CER complements the NIS2 and reinforces the resilience of pan-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 member states to undertake risk assessment on a regular basis to identify entities that are critical or vital for the economy and functioning of civil society.

Digital Operations Resilience Act (DORA) – Regulation (EU) 2022/2554

The Digital Operations Resilience Act (DORA) will come into force in 2025, it was approved on 22.11.2022 at the European Parliament's plenary session. DORA seeks to harmonise, and improve, operational resilience in European financial services. It seeks to ensure that the EU's financial sector is resilient to cyberattack/strikes and operational disruptions. Thus, banks, crypto-asset service providers, electronic money providers, investment firms, payment providers and third-party ICT providers will be subject to the new rules. Supervision, enforcement, and implementation is delegated to national authorities.

2. The Impact of NIS2

What follows is a brief overview of some of the changes to be ushered in under the NIS2.

Expansion in Scope and Detail

The NIS in its current form was the first pan-EU legislation focused on cybersecurity and was adopted in 2016. Its aim, like other legislation, was to create a harmonised level of cybersecurity throughout the EU. Thus, it required operators of 'essential services' to implement risk management and undertake reporting obligations; these included health and energy entities, transport, and infrastructure businesses, as well as those offering digital service such as cloud computing or search engines facilities etc.

The NIS2 changes this, its perspective builds on 'essential' entities adding those considered 'important', and its sectoral application is far wider. Organizations not previously falling within the ambit of the NIS may fall into the remit of NIS2. The full list is set out in Annex I ('essential') and Annex II ('important') of the NIS2. These are as follows:

Essential (emphasis added)

- *Banking*
- Energy
- Drinking Water
- *Digital Services / Infrastructure*
- *Financial Markets Infrastructure*
- Health
- Public Services (not including the judiciary, parliament and central banks)
- Transport

- Space

Important (emphasis added)

- Couriers
- Chemical Distribution
- 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
- Research
- Waste Management.

This exact scope will only be fully appreciable when NIS2 is implemented. NIS2 also provides more detail on the entities within various sectors that are subject to the proposed law. At present the member state would be tasked in creating a list of those that are subject to the NIS, the NIS2 creates cap (size) so that all relevant medium and large entities would have to comply with the Directive. Furthermore, NIS2 applies to those considered essential and important regardless of their respective size if, they provide public electronic communications networks/services, where potential disruption of a service offered could impact on safety of the public, security or health, and where potential disruption of a service offered could cause systemic risk, especially in those sectors where a cross-border ripple effect could occur. In addition, designation as essential or important, where the size threshold is not met, can take place where it is the sole provider of a service critical to economic or social activity. It should be noted that member states have until 04.2025 to determine a list of essential and important entities subject to the NIS2.

Increased Liability for Cybersecurity Risk Management – Corporate Accountability

NIS2 increases the responsibility that 'management bodies' (MB) must bear in ensuring compliance with the NIS2. Thus, when a member state implements the NIS2 it must ensure that those MBs do the following:

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

Practically, this renders the MB liable where the entity breaches the NIS2. The effect of these requirements elevates the responsibility of managing cybersecurity risk to the remit of senior management. Thus, the MB is ultimately responsible, and a dereliction of duty could result in management being held liable for breaches and fines – subject to those set out in the legislation passed by the member state in adoption of the NIS2 into their respective legal systems. In addition, the NIS2 leaves it to the member state to define what amounts to a MB, the term is not defined, other than suggesting that individual(s) that discharge managerial functions could

well constitute a MB for the purposes of the Directive. Thus, an MB is likely to include the board of directors and particular company executives. Equally, it would be the same individual(s) who would be the subject of any subsequent enforcement action that is taken for the entity's failure(s) to comply with the NIS2. For example, member state legislation, when adopting the NIS2, permits individuals at a senior level (C-Suite) to be banned from continuing to discharge managerial functions, until deficiencies have been remedied and/or compliance with requirements as set out by a competent member state authority (as designated) is achieved. The NIS2 also facilitates member state requests that entities in breach make a statement (public) regarding the occurrence of an infringement but also name those responsible for it. This is obviously designed to pose a reputational risk to the entity and deter non-compliance. Whether this latter objective will have desired effect is debatable, given this is like actions taken by financial regulators when imposing fines on financial entities, the sophisticated communication management teams, that navigate such risks with relative ease. The NIS2 does not delimit the member state from legislating appropriate penalties, but they must be dissuasive, effective, and proportionate. This means that they may, as the NIS2 (Recitals) makes clear, include criminal punishment. Thus, from a compliance perspective the entity must be aware of any civil and/or criminal penalties that exist in the respective jurisdictional legislation that transposes the NIS2 into their domestic law.

Expansion of Reporting Requirements – 3-Tier Approach

The NIS2 streamlines reporting obligations, it is more precise than its predecessor (NIS) in providing precise provisions relating to reporting, report content and timeframes. Essential, and important entities must notify the member state 'competent authority' or a 'Computer Security Incident Response Team' of any incident of *significant impact* on the services they are providing or the recipients of those services. This includes an incident that has caused or can potentially cause disruption to operations or loss (financial) that is substantial. This also covers cybersecurity threats/strikes that could have resulted in the occurrence of a significant incident. The NIS2 moves to a 3-tier approach as follows:

- Tier 1: early warning, notify within 24-hours of becoming aware of the incident. This is a move away from reporting 'without undue delay' under the NIS, to an initial notification requirement.
- Tier 2: intermediate notification, undertaken within 72-hours of the entity becoming aware of the incident. It must also provide an initial assessment of incident impact and severity, and any indicators of compromise.
- Tier 3: final report, submitted within 1-month of the incident notification, it must include a detailed report of the incident and its cause.

If an incident reported under the NIS2 Directive involves personal data, then it would almost certainly fall foul of the EU General Data Protection Regulation 2016/679 (GDPR) and thus, the NIS2 states that the 'competent authority' must also inform the relevant 'data protection authority' of any incident that would amount to a notifiable breach of personal data. Interestingly, where a fine is imposed by the data protection authority for a violation of the GDPR then the NIS2 competent authority is prohibited from imposing a financial penalty for the same incident. This prevents the entity from being penalised twice for the same incident. Whilst the financial penalty is restricted in this way, the NIS2 competent authority may still impose any other non-financial penalties it has at its disposal i.e., adhering to deadlines for rectifications resulting from a cybersecurity audit or publish details about the infringement.

Cybersecurity Risk Management Measures – Key Measures

The NIS2 provides a streamlined cybersecurity management approach, this is designed to reduce resilience inconsistencies across all relevant sectors. Thus, it introduces key measures that all entities subject to the NIS2 must undertake to manage cybersecurity risks relating to their networks and information systems, these are:

- Business continuity and management of crises.
- Cryptography and encryption.
- Frameworks/process to assess the effectiveness of their cybersecurity 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 and security of information systems.
- Security in the supply chain; data storage, key relationships with its suppliers etc.

Competent Authorities and Enforcement Powers

Essential and important entities will be subject to supervision from a competent authority within the jurisdiction in which they are established or where cloud computing and digital infrastructure providers are concerned, the jurisdiction is where their 'main EU establishment' (ME) is located. The ME is the place where decisions on cybersecurity risk-management measures are taken, where that cannot be determined or if those decisions are taken outside of the EU, then the ME will be the location within the EU in which the entity's cybersecurity operations are undertaken. If, even at that point it cannot be determined which member state has jurisdiction, then the ME will be the member state in which the entity has the greatest number of EU employees. Those entities that are established in a non-EU jurisdiction are required to designate an EU representative in any EU member state in which they offer their services. The regime of supervision and enforcement penalties afforded to national (competent) authorities under the NIS2 are far more detailed than those set out in NIS. The authority may do as follows:

- Undertake on-site security audits and inspections.
- Make requests for information so that it can assess an entity's cybersecurity measures.
- Carry out security scans.
- Make requests for access to information to facilitate assessment of cybersecurity risk-management measures, to determine the level of implementation of data and policies etc.

There is a difference in terms of investigation between essential and important entities. The NIS2 Directive allows the investigation of essential entities at any time, whether regularised or random. In contrast, important entities can only be investing after an incident has occurred (*ex-post*). For breach of cybersecurity risk management measures or incident reporting obligations, the NIS2 permits the implementation of administrative fines for essential entities at a minimum of 10M€ (as stated earlier), or 2% of global turnover for the previous financial year – the greater of the two figures wins. The equivalent for important entities is 7M€ or 1.4% of global turnover, again the greater of the two figures. Additionally, the competent authority may impose non-financial remedies such as orders to comply, implement cybersecurity audit findings, to inform stakeholders and to make public information.

3. UK – EU Contrast

Whilst the UK and EU have aligned their respective regimes since the UK withdrew from the EU, the evidence suggests there will be some divergence in terms of the approach to the regulation of critical cybersecurity infrastructure where the two are concerned.

Digital or managed service providers are being brought into the regulatory gaze in the UK and EU. If it chooses, like the EU, the UK government can bring 'other' sectors it believes to be critical into the scope of its regulations with greater ease. The financial sector, in the UK, is not subject to the NIS is facing additional regulatory requirements from the PS2/21 (Solvency II)[14] and Financial Services and Markets Bill[15] which seeks to manage deterioration of service, supplier failure and concentration risk.

In the UK, entities that are regulated by the NIS will need to continue to implement cybersecurity measures the sectorial competent authorities require them to. Albeit the UK government has indicated that for greater flexibility it would seek to promote a tool kit approach, such as the Cyber Assessment Framework[16].

The UK is also updating reporting requirements, the definition of 'incident' is to 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.'[17]

In terms of compliance, the UK provides for fines of up to £17M and unlike the EU there is no option for this to be equivalent to 2% of total worldwide turnover etc.

4. Conclusion and Practical Steps

The NIS2 must be implemented by member states by 18.10.2024, and thus EU businesses need to start considering the following if they have not done so already:

- Ascertain whether the NIS2 covers the services or activities they provide, and if it does, which companies or subsidiaries are affected.
- Begin assessing their security controls and amend polices/processes as necessary.
- Prepare/amend plans/policies from a financial, organisational, and technical perspective to achieve compliance.
- Plan documented processes in anticipation of due diligence.
- Ensure that changes, controls, and incident response measure obligations are communicated with suppliers to address supply chain risk, and reporting requirements.
- Prepare an ICT plan, as the EC expects the NIS2 to create additional spend of over 20 – 22% for entities not subject to the current NIS but subject to the NIS2, and a conservative 10 – 12% for those that already comply with the current NIS regime.

[14] 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.
[15] Financial Services Future Regulatory Framework Review: Proposals for Reform, 2021. UK: HMSO.
[16] 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
[17] Government response to the call for views on proposals to improve the UK's cyber resilience. Consultation Outcome, 30 November 2022. UK: HMSO. See para. 5.4.

UK entities must still appreciate which regulations they are subject to including the UK's own currently evolving regulatory regime. Unlike the NIS2 which came into force in January 2023, and given the restrictions on UK parliamentary priorities and an upcoming general election, it is unlikely that the current UK regime is going to be updated any time soon, not least before 2024/25.

*Dr. Charanjit Singh, Tenant and Barrister-at-Law at Holborn Chambers, and PhD – University of Southampton.

Email: C.Singh1@westminster.ac.uk