The European Union (EU) Network Information Security Directive 2.0 (EU NIS 2.0)

Implementing a high common level of cybersecurity across the EU

January 2023

Andy Watkin-Child and Jaime Foster

HILL DICKINSON

PARAVA
CYBER CONSULTING

European Union (EU) Cybersecurity Risk Management Regulation

Network Infrastructure Security Directive 2.0 (EU NIS 2.0)

The EU has passed regulations to strengthen the resilience of EU Member States' Critical National Infrastructure (CNI). These regulations implement an integrated harmonized regime for cybersecurity risk management, these include the *Digital Operational Resilience Act* (DORA 2022/2554) for the financial sector, *The Network Infrastructure Security Directive 2.0* (EU NIS 2.0 2022/2055 -'The Directive') for CNI, *The Resilience of Critical Entities* Directive (EU 2022/2557) for CNI and the proposed *Cyber Resilience Act* 2022/0272 (COD) for the security of hardware products and services.

The purpose of this paper is to focus on one aspect of the forthcoming regulations, the Network Infrastructure Security Directive 2.0.

What is Critical National Infrastructure (CNI)?

CNI sectors deliver services that are indispensable for the maintenance of vital societal functions and the economic activities of governments and their national markets. CNI sectors include energy, transport, banking, water, agriculture, production, food processing and distribution, health, financial market infrastructure, digital infrastructure, public administration, and space. Managing the growing interdependencies between CNI is critical for the effective, safe, and secure operation of the EU and its Member States.

The EU aims to support the protection of critical infrastructure across the Union through regulation, that to date has been hampered by diverging regulatory cybersecurity requirements, inconsistent cyber laws, varying levels of resilience and regulatory duplication. Creating unnecessary administrative burden for companies operating across boarders leading the EU to revise EU NIS 1 (EU 2016/1148).

The Directive lays down harmonised minimum rules for the cybersecurity of essential services, deemed critical for the proper functioning of the EUs internal market. The EU Commission recognizes that CNI organisations need to better manage the risks to their operations that may disrupt the delivery of essential services. A recognition that has been clarified following cyber-attacks across the U.S and EU in 2021 and 2022, which demonstrate CNI sectors are at increased risk of cyber-attack and the cybersecurity maturity of CNI providers maybe insufficient to deal with emerging threats. The EU recognises the potential social and economic impact of a cyber-attack on CNI and its customers and the economic ramifications, and societal impact of a systemic cyber-attack.

The Directive – Its aim?

The Directive was published in the EUs official journal on the 14th of December 2022 and took effect from the 17th of January 2023. Member states now have 21 months to transpose the Directive into their national laws. The Directive should be read in conjunction with '*The Resilience of Critical Entities*' (EU 2022/2557), the EU '*Digital Operational Resilience Act – DORA'* (EU 2022/2554) published on the 14th December 2022 and the proposed EU '*Cyber Resilience Act (CRA)'* (2022/0272 (COD)).

The Directive sets out to create an integrated harmonised regime for cybersecurity risk management, for EU Member States to codify into law. The Directive lays down requirements for

the cybersecurity risk management of entities covered under the scope of application, and measures that aim to achieve a high common baseline of cybersecurity across the Union. The Directive sets out obligations for Member States to adopt:

- A national cybersecurity strategy, designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity, and Computer Security Incident Response Teams (CSIRTs).
- Cybersecurity risk-management measures and reporting obligations for entities of a type referred to in the Directive Annex I or II, as well as for entities identified as critical entities under Directive (EU) 2022/2557.
- Rules and obligations on cybersecurity information sharing.
- Supervisory, reporting and enforcement obligations.

The Directive – Scope

The scope of the Directive is split between two groups. Those entities in sectors deemed '*sectors of high criticality - Directive Annex I'*, that includes energy (electricity, district heating and cooling, oil, gas, hydrogen), transport (air, rail, water, road), banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, ICT service management, public administration, and space. The second group consists of '*other critical sectors – Directive Annex II'*, that includes postal and courier services, waste management, manufacturing, production and distribution of chemicals, production, processing and distribution of food, manufacturing, digital providers, and research organisations.

The Directive applies to both public and private entities within *sectors of high criticality* and *other critical sectors,* whose turnover is between Eur 10 Mn and Eur 50 Mn and who employ between 51 and 250 persons and/ or have an annual balance sheet of between Eur 10 Mn and Eur 43 Mn. The directive also applies to organisations whose turnover is greater than Eur 50 Mn, employ more the 250 persons and/ or whose balance sheet is greater than Eur 43 Mn.

Regardless of size, the Directive also applies to entities that provide public electronic communication networks, publicly available electronic communications services, trust service providers, top-level domain name registries and domain name system service providers, domain registration services, entities that are the sole provider of essential services for the maintenance of critical societal economic services, entities where the disruption of services could have a significant impact on public safety, security, health or induce significant systemic risk for a sector, the entity is a public administration entity of central government, regional or local level, education institutions where they carry out critical research, critical entities defined under EU 2022/2557.

The Directive - Implementation by '*Member States'*

The success of the Directive in harmonising cybersecurity, relies upon Member States implementing appropriate strategic, governance, policy, resourcing, oversight and assurance, and reporting infrastructure. The Directive sets out the requirements for Member States to adopt a national cybersecurity strategy, with coherent strategic objectives, policies to deliver the strategy and appropriate governance to oversight and assure its implementation. With a view to collaborating with other Member States, the EU Commission, Council, and agencies such as ENISA (the European Union Agency for Cybersecurity) and harmonizing the management of cybersecurity nationally and across the EU Member States.

The Directive lays out some notable requirements for the EU Commission and Member States to:

- Harmonise cybersecurity risk management measures and reporting obligations between existing sector specific Union legal acts and the Directive.
- Designate or establish one or more competent authorities, responsible for the application of the Directive and cross border cooperation.
- Acknowledge EU DORA, the CRA and incident reporting over the Directive.
- Comprehensively address the cybersecurity risk management obligations of digital infrastructure, DNS, TLD registries, ICT service and cloud service and data centre providers. Promote the use of certified ICT products, services, and processes ahead of the introduction of a cybersecurity certification scheme, proposed by EU 2022/0272 (COD).
- Address both physical and logical security provisions as part of cybersecurity risk management measures and reporting obligations.
- Contribute to the establishment of the EU Cybersecurity Crisis Response Framework, set out under EU 2017/1584. Establish one or more Computer Security Incident Response Teams (CSIRTS) to monitor critical entities.
- Foster alignment with international standards and best practices for cybersecurity risk management.
- Adopt cybersecurity risk management practices, measures, and risk mitigations by covered CNI entities, that are proportionate to an entity's exposure to risk and the societal and economic impact a cyber incident could have.
- Report cyber events to the National CSIRTs within 24 hours.
- Introduce comprehensive risk-based *ex ante* and *ex post* on and off-site supervision of entities.
- Implement a Civil and Criminal penalty regime for failing to comply with the Directive. Penalties that include fines against entities and persons; the temporary suspension of natural persons responsible for failing to discharge their managerial responsibilities defined by the Directive.

The Directive - Implementation by '*CNI Entities of Member States*'

Cybersecurity Risk Management, Governance, Measures and Reporting Obligations

The products and services that are produced by the CNI sectors in scope, are critical to Member State national security and the security of the EU. The Directive requires Member States to create laws for the management bodies (legally defined accountable representatives) of covered entities to approve their organisation's cybersecurity risk-management measures.

Member States are required to ensure that management bodies of covered entities undertake cybersecurity risk management training and are encouraged to offer similar training to their employees. The learning objective is to provide sufficient knowledge and skill enabling the management bodies of covered entities to oversee and assure cybersecurity risk-management, treating the impact of cyber risk on the services they provide.

The implications of these requirements are that the boards of covered entities must implement appropriate corporate governance processes for the oversight and assurance of cybersecurity risks, evaluate control effectiveness and attest to the effectiveness of the risk treatments performed. Boards need to have oversight and assurance of cybersecurity risks in line with changes in business strategy, financial plans, changes in operational performance and changes in an entities threat profile.

Covered entities will be expected to follow a proportionate approach to the cybersecurity risk management of their network, systems and physical environment based upon their size and type. Including at a minimum:

1. Policies on risk analysis and information systems security.
2. Incident handling.
3. Business continuity, backup management, disaster recovery and crisis management.
4. Supply chain security, including the security of relationships between entity direct supplier and service providers.
5. Secure acquisition.
6. Policies and procedure to assess the effectiveness of cybersecurity risk management measures.
7. Policies and procedures regarding the use of cryptography.
8. Basic cyber hygiene and cybersecurity training.
9. Human Resources security.
10. Multi Factor Authentication.

Where entities do not comply to these requirements Member States shall ensure that all necessary, appropriate, and proportionate corrective measures are taken by the entity without undue delay.

Reporting Obligations

In scope entities must report any incident that has a significant impact on the provision of their services. That by causing or can cause severe operational disruption of their services, financial loss for the entity concerned, or has affected or can affect other natural or legal persons by causing considerable material or non-material damage. To their Member State CSIRT or competent authority within 24 hours of becoming aware of the incident and to their customers.

Cybersecurity Certification Schemes

Member States may require covered entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881.

Supervisory and enforcement

The Directive requires in scope organisations to take appropriate and proportionate measures to manage cybersecurity risks. Member States are to oversight and assure the compliance of in scope entities, ensuring that competent authorities provide the necessary compliance oversight and assurance. When exercising their supervisory tasks in relation to essential entities, competent authorities will have the power to subject those entities to at least:

1. On-site inspections and off-site supervision, including random checks.
2. Regular and targeted security audits carried out by an independent body or competent authority.
3. Ad hoc audits, on the ground of a significant incident or an infringement of this Directive
4. Security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria.
5. Requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned.
6. Requests to access data, documents, and information necessary to carry out their supervisory tasks.
7. Requests for evidence of implementation of cybersecurity policies.

Member States shall ensure that the competent authorities have the powers to issue infringement warnings and set compliance deadlines for entities to adopt binding instructions to prevent of

remediate incidents; order entities to cease conduct and desist from repeat conduct; order entities to comply with cybersecurity risk management measures; order entities to inform their clients of potential significant cyber threats; to implement recommendations following security audits; to make public aspects of infringements of the Directive, and issue fines.

Member States are to ensure that the person acting as the legal representative of a covered entity with authority to take decisions on its behalf, or authority to exercise control of it, has the power to ensure compliance with the directive can be held liable for breach of their duty if the directive is not complied with.

Where enforcement measures are ineffective Member States shall ensure that competent authorises have the power to establish compliance deadlines. Where requested actions are not taken within set deadlines Member States are to ensure competent authorities can

- Suspend temporarily a certificate or authorisation concerning all or part of the relevant service provided, or activities carried out by the entity.
- Prohibit temporarily any natural person which is responsible for discharging managerial responsibilities from exercising managerial functions in the entity.
- Impose administrative fines.

Administrative fines for covered entities that do not comply with the appropriate cybersecurity risk management, oversight and assurance can vary. Entities considered '*essential*' can face fines of a maximum of at least EUR 10,000,000 or of a maximum of at least 2% of the total worldwide turnover from the preceding financial year, whichever is bigger. For entities that are considered '*important*' a maximum of at least EUR 7,000,000 or of a maximum of at least 1.4% of the total worldwide turnover from the preceding financial year, whichever is bigger.

The Directive - What does this mean in practice?

Businesses covered under the scope and their suppliers should consider upgrading their compliance programmes in preparation of Member States transposing the Directive into national laws to provide assurance of compliance. Businesses should consider the requirement to "take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services". Businesses should also be able to provide oversight and assurance of the risks and their treatment.

Clearly, the UK will not need to transpose the Directive, and it remains to be seen how the government will implement the outcome of its consultation on proposals to improve the UK's cyber resilience, including by updating the current Network and Information Systems Regulations 2018 (SI 2018/506) (NIS Regulations). The government has announced that it will proceed with these proposals and amend the NIS Regulations accordingly, subject to finding a suitable legislative vehicle.

Cyber security remains a burning issue. Research by the Department for Digital, Culture, Media and Sport shows only 12 per cent of organisations review the cyber security risks coming from their immediate suppliers and only one in twenty firms (5 per cent) address the vulnerabilities in their wider supply chain.

Assuming UK law continues to implement enhanced cyber security requirements for businesses, the following are also important to consider from a legal perspective:

Regulatory compliance

While the Directive will have a significant impact on UK firms, it is by no means the only cyber compliance issue to be dealt with. The U.S Securities and Exchange Commission (SEC) is proposing cyber regulation that will impact organisations seeking access to U.S capital markets, the DoD is implementing DFARS and CMMC across the global Defence Industry Base (DIB) and the Office of the National Cybersecurity Director is implementing a U.S National Cyber Strategy.

The International Maritime Organisation has mandated that ship owners and managers must incorporate cyber risk management and security into the ISM Code safety management on vessels. Similarly, NHS Digital's Data Security and Protection Toolkit Assessment requires NHS bodies to have strategies in place to protect IT systems from cyber threats based on proven cyber security frameworks.

A UK regulator of relevance is the Financial Conduct Authority (FCA) which has responsibility for countering financial crime, which results several requirements on firms relating to cyber security, set out in the FCA Handbook. Requiring firms to have effective, proportionate and risk-based systems and controls in place to ensure they cannot be used for financial crime.

Article 33 of the UK GDPR also requires companies to ensure they have an 'appropriate level of security' that safeguards personal data and alert the Information Commissioner's Office within 72 hours of a data breach. Businesses must constantly consider and re-consider how to comply with this requirement.

Litigation

There is a marked increase in cyber litigation ("right of bang"). Businesses may find that they have limited recourse to their customer and suppliers when cyber issues arise, and it has become increasingly apparent that they must be proactive in ensuring contractual terms give them remedies in this situation.

Examples where litigation may be necessary include:

- Defending organisations against government regulators and data protection authorities.
- Defending privacy claims for data protection infringement (including breaches of the GDPR and PECR (cookies and similar technologies claims)), misuse of information, negligence, breach of trust and confidentiality claims.
- Helping organisations start litigation proceedings against any third parties who contribute to a cyber incident.
- Cyber security fraud where suppliers are alleged to knowingly conceal cyber security problems.
- Breaches in contract that arise for failing to comply with requirements to implement cybersecurity. Breach in contract for failing to deliver products and services that arise from cyber-attacks.

Commercial

Commercial contracts increasingly include terms requiring compliance with Cyber requirements. For example, the UK government's Model Services Contract requires higher-risk subcontractors to be

certified to ISO/IEC 27001 and/or to possess Cyber Essentials Plus certification. The U.S DoD implemented DFARS 252.204-7012 that requires all covered Defense contractors globally to implement NIST SP 800-171.

Corporate

Performing effective 'Cyber due diligence' is vital for businesses looking to merge with/acquire a new company - a purchaser should know the target company's internal processes to ensure it understands their cybersecurity risks and policies. This would include considering:

- Is the deal involving a high-risk target?
- If a large amount of personal or sensitive data is being held, what are the target company's data protection compliance and processes?
- What are the data assets held by the target company?
- Has the target company undertaken any third-party audits to show it has sufficient cyber risk management if place? If not, do we need to undertake our own audit?

Insurance

In addition to any war exclusions clauses, insurance companies are introducing clauses to exclude insurance losses that result from state backed cyber-attacks. This places more burden on companies as the traditional mechanism for mitigating cyber risks that is cyber insurance is less likely to mitigate the risk and require organisations to manage cyber security risks 'Left of bang'.

Insured companies, and their insurers, may be required to investigate fraud and the trace and recover funds that have been wrongfully diverted to third party accounts following a cyber security incident. Insurers also need to consider how to approach issues of coverage where an insured party has been found not to have performed its commercial or regulatory following a cybersecurity incident.

Governance and employment

Under the Directive, Management bodies must "approve the cybersecurity risk management measures taken" and oversee their implementation. Individuals in those bodies could be held personally liable if the organisation fails to comply with its cybersecurity obligations under the legislation. This requires careful consideration.

Board composition to incorporate Cyber security expertise is fast becoming an organisational priority. For example, in the US the SEC have proposed new rules requiring companies to show they have appointed a director to their Board who has cyber security expertise. Such expertise may be determined by whether the director in question has experience or qualifications in cyber security, and this requirement may soon be replicated in the UK.