Ibec position on NIS2

Cybersecurity – Review of EU rules on the security of network and information systems

March 19, 2021

Contents

Introduction

Ibec believe cyber security and cyber resilience are economic and social imperatives for Ireland and Europe. The pandemic greatly accelerated the economic and societal imperative for digitally enabled transformation of government and public services, enterprise, and human interaction by several years. As a digitalised economy and society, we must preserve trust online and protect our people, businesses, services, and critical infrastructure.

Ibec[i] welcomes the opportunity to respond to this consultation[ii]. We acknowledge the Directive on the security of network and information systems (NIS Directive[iii]) as an important piece of EU legislation that aimed to improve and harmonise Europe's cybersecurity preparedness at national and EU level. We understand the proposed revision ('NIS 2'), currently under discussion by the EU's co-legislators, hopes to deepen that preparedness. In this context, we would like to highlight Ibec recommendations for future discussions on the file, including:

1. Provide further clarity on the scope of the proposal.
2. Ensure regulatory consistency. Deepen preparedness and harmonise cyber security and resilience across the EU.
3. Ensure obligations offer flexibility and are proportionate and technically feasible.
4. Proposed enforcement and sanctions should be proportionate and contextual.

Recommendations

a. Scope

Provide further clarity on the scope of the proposal. We acknowledge that the pandemic has shown the need to broaden and deepen cyber security efforts. We understand the desire to expand the list of entities considered as an Operator of Essential Services (OES) and important entities[iv] to respond to changes in the cyber threat landscape and to bring greater harmonization and further legal clarity to organisations. However, we need to get the balance right and ensure a proportionate, risk-based approach.

Recommendations:

- **Provide a more granular assessment of risk and further clarity on what types of entities should be considered important**. The scope of the proposal on manufacturing[v] appears very broad and likely to include almost all manufacturing. In addition, the current scope does not appear to take account of differences in B2B and B2C relations and risks they are carrying.

- **Support harmonisation and the exclusion of non-essential micro-small entities**[vi]. Nevertheless, the NIS 2 should consider including incentives, for example funding and education, for SMEs to uptake cybersecurity measures. Under Recital 9, Member States could also produce a definition criterion to establish what SMEs would be critical or important. There is potential for fragmentation and uncertainty for SMEs

operating in multiple Member States as they may be within scope in one Member State but not another.

- **Conduct risk-based assessments of supply chain security for certain technologies**[vii]. This approach could help exclude SMEs but ensure technology/ technological services they may provide and deemed to be critical to an OES is assessed. While software providers cannot control exactly how businesses will use their services, some graded risk-based due diligence and information sharing obligations could be useful. Clarify responsibilities of different entities of the supply chain. Entities should only be responsible for the obligations that are under their control.

b. Consistency

Support the broad aim of deepening preparedness and harmonisation on cyber security and resilience across the EU. We are stronger if we act together and consistently to this shared challenge.

Recommendations:

- **The Commission should publish guidance.** Help preparedness and ensure harmonization in implementation across Member States.
- **Ensure coherence with broader regulatory requirements**. The expansion of the NIS 2 scope means the inclusion of entities subject to parallel regulation with additional reporting requirements. For example, the European Electronic Communications Code (EECC), the proposed Digital Operational Resilience for the Financial Sector Regulation (DORA), General Data Protection Regulation (GDPR) and Payment Services in the internal market Directive (PSD2). Potentially an OES or Important Entity may have to report a data security incident, involving personal data, to several separate authorities with different requirements. Horizontal and sectoral legal instruments should be sufficiently aligned, and additional regulatory overlaps/burdens avoided.

c. Obligations

Ensure obligations offer flexibility and are proportionate as well as technically feasible. Take a risk-based and outcome-based approach.

Recommendations:

- **Entities should be allowed the flexibility to adopt security safeguards and measures that they deem fit for purpose**. For example, mandating a specific form of encryption potentially closes the doors for entities implementing new or more advanced solutions to achieve the desired outcomes and enable agility in responding to evolving threats, a more technology neutral approach is needed. Recital 54 should be clarified that no backdoors are mandated.

- **Facilitate the further uptake of international standards for risk-management**[viii] **across the economy**. Deepen EU co-funding supports in cybersecurity.
- **Retain a voluntarist approach to certification.**
- **Provide practical guidance on risk management obligations.** Obligations in Art 18(2) are very detailed and could lead to disproportionate burdens for some businesses. This removes discretion as to how this duty of care should be offered by certain businesses depending on their risk profile. Furthermore, the list of required obligations does not depict how compliance with them can be properly demonstrated. Businesses will also be responsible for others in their supply chains. Art 18(3) worryingly obliges businesses to take account of vulnerabilities specific to each supplier and services provider in their supply chain. This will not be realistic for many businesses who will fall under this NIS 2.0 Directive as they exist within large global supply chains where they have little or no control over other businesses that operate within them.

- **Ensure proportionality and technical feasibility in reporting requirements**.
    - Art 20(2) obliges businesses to notify CSIRTs of significant cyber "threats" that could result in a "significant incident". The obligation to report potential future events – detached from any parameters regarding likelihood/certainty, and/or foreseeability of the future event arising - appears unreasonable and even difficult to demonstrate compliance. It is far from clear as to when a threat becomes significant and offers little cybersecurity capacity building.
    - Art 18(3) obliges businesses to inform customers. This could cause unnecessary distrust of digitalisation on a wider scale once the incident has been solved. Therefore, we believe information should only be sent to customers impacted in a private manner.
    - Art 20(4)(a) obliges all entities covered by the NIS 2.0 Directive to report incidents "without undue delay". While the notification itself could be a straightforward procedure if national authorities have sufficient one stop shop systems, the 24-hour reporting period does not consider the need for the business to perform a sufficient analysis to determine whether the threshold for notification is reached. Further to this, the focus following an incident should primarily be mitigation. In the interests of cybersecurity capacities and proportionality, we would urge the co-legislator to extend this current period to 72 hours.
    - Proposals for a European vulnerability register should align with security best-practices surrounding vulnerability disclosure. The experiences gained through the development of other similar initiatives such as the Common Vulnerabilities and Exposure (CVE)[ix] database or the NIST National Vulnerability Database (NVD)[x] should be leveraged. We are unclear as to whether entities must report vulnerabilities to ENISA or national CSIRTs and whether 3rd country reporting is still permitted. Art 6 should only make vulnerabilities public if mitigation knowledge is available, and with sufficient safeguards to enable confidential and/or business sensitive information to be protected. A clear deadline should be included so that businesses have sufficient time to fix the vulnerability. Avoid references to businesses reporting the vulnerabilities.

d. Enforcement

Proposed enforcement and sanctions should be proportionate and contextual. The NIS2 proposes significant potential administrative fines to entities deemed 'essential and important'. The approach appears reflective of the GDPR approach.

Recommendations:

- **It is important that proposed enforcement and sanctions remain proportionate** and take into consideration the specificities of each individual case and encourage entities who continue to act in good faith.
- **We encourage the Cooperation Group to actively engage and cooperate with OESs and Important Entities**. Business will continue to invest in cyber security and cyber resilience. Collaboration between business and authorities, rather than sanctions should be the primary route to achieve the shared goals.
- **The NIS2 should introduce an incentive-oriented approach** to stimulate cybersecurity resilience and not prevent innovation through fines.
- **The proposed NIS2 review underlines the need to deepen investment in national data security capacities**. We encourage the resourcing and implementation of National Cyber Security Strategies. We must deepen our cybersecurity ecosystem and ensure our national cyber security capacities are adequately resourced.

Endnotes

[i] Ibec www.ibec.ie/digitalpolicy

[ii] National consultation on the proposed revision to the Directive on Security of Network and Information Systems (NIS Directive), open till March 19, 2021

[iii] NIS Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[iv] Previously considered as Digital Service Providers.

[v] Section 5 of Annex II

[vi] Recital 8

[vii] See Recital 43, 46, 47 and Article 5.2(a), Article 18.2 (d) and Article 19 of the proposal

[viii] For example, ISO/IEC 27001

[ix] http://cve.mitre.org/

[x] https://nvd.nist.gov/