AmCham EU

SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Fragmented implementation of the NIS2 transposition

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3.7 trillion in 2022, directly supports more than 4.9 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

Executive summary

The transposition of the Directive on measures for a high common level of cybersecurity across the Union (the NIS2 Directive) represents a pivotal moment for enhancing cybersecurity across the EU. However, the significant flexibility granted to Member States in implementing the Directive has led to a fragmented regulatory landscape. This fragmentation undermines the Directive's core objectives, creating operational and compliance challenges for pan-European service providers and hindering the EU's ambition for a harmonised digital single market.

Key issues include diverging national requirements that increase compliance costs and administrative burdens, reduced competitiveness for pan-European operators and diminished effectiveness of the NIS2 framework. Specific areas of concern include discrepancies in reporting obligations, definitions of scope and security audit requirements, as well as the interplay with sector-specific regulations.

This paper emphasises the need for harmonised implementation, leveraging international standards and fostering mutual recognition of audits to reduce duplication and complexity. It also advocates for proactive guidance from the European Commission to ensure consistent transposition across Member States. By addressing these challenges, the EU can maximise NIS2's potential, fostering a resilient and unified cybersecurity environment while promoting competitiveness and innovation.

Introduction

The NIS2 Directive represents a crucial step towards enhanced cybersecurity within the EU. However, the flexibility afforded to Member States risks undermining this progress, resulting in a fragmented regulatory landscape. This fragmentation poses a significant threat to the Directive's effectiveness and places a disproportionate burden on pan-European providers. The new Commission can and should address this issue, especially taking into account the overarching intention for regulatory simplification in the 2024-2029 mandate.

Diverging national requirements: a barrier to a unified cybersecurity landscape

While the NIS2 Directive aims to create a harmonised cybersecurity framework across the EU, the transposition process grants Member States significant leeway in interpreting and implementing its provisions. These discrepancies pose significant challenges for organisations operating across multiple Member States, which struggle to navigate a complex web of diverging requirements, potentially increasing compliance costs and creating an uneven cybersecurity landscape within the EU. Significant hurdles for pan-European providers include:

- **Disproportionate burden.** Navigating a complex web of national requirements strains resources and stifles innovation. The need to comply with multiple, potentially overlapping regulations diverts time and resources away from core business operations and cybersecurity enhancements. This affects the cost of finding implementation solutions that are suitable to all the competing national regulations and creates friction due to the need to develop supporting audits for each of these national regulations. Global enterprise security functions may be redundantly audited by different Member State authorities, including within the same Member State, due to the lack of agency coordination and recognition.

- **Reduced competitiveness.** Increased compliance costs and complexity, without a corresponding improvement in security decision-making, put pan-European providers at a competitive disadvantage compared to entities operating solely within less regulated Member States.
- **Barrier to the Single Market.** Divergent requirements create unnecessary obstacles for companies operating across borders, hindering the free flow of services and potentially fragmenting the digital single market. This runs counter to the principles of a unified digital space within the EU.
- **Reduced effectiveness of NIS2.** The administrative burden associated with compliance can overshadow the Directive's core objective of enhancing cybersecurity. Instead of focusing on proactive measures and long-term strategies to counter emerging threats, organisations can become bogged down in navigating and adhering to a complex regulatory maze. Competing regulations and differences between NIS2 implementation across the EU can lead to conflicting security positions from competent cybersecurity authorities. This diverts organisations from executing security to coordinating between agencies on an appropriate approach. In addition, prescriptive security requirements from Member States can weaken effective security as they may not suitably address risks a specific organisation faces.

This flexibility for Member States has led to a fragmented landscape of national requirements, as highlighted by the early and not fully aligned transposition efforts of Belgium, Croatia and Hungary, as well as the various draft proposals put forward in other Member States and recognised by the European Union Agency for Cybersecurity (ENISA) in its *2024 Report on the State of Cybersecurity in the Union*.[1] Areas exhibiting variations in national interpretations include, among others, scope, reporting, audits and certifications.

This fragmentation echoes concerns raised in reports like Enrico Letta's *Much More Than a Market*, which highlights how 'fragmentation in rules and industries at the National level hinders a crucial final step towards a Single Market for Electronic Communications'.

Towards a harmonised cybersecurity approach

To fully realise NIS2's potential and achieve a truly robust cybersecurity landscape within the EU, addressing this fragmentation is crucial. Member States must strive for greater harmonisation of national requirements, ensuring consistency and interoperability across borders and encouraging the

[1] ENISA, *2024 Report on the State of Cybersecurity In the Union*, December 2024

adoption of existing, widely recognised, international standards to streamline compliance and reduce unnecessary duplication of efforts. ENISA has already highlighted the benefits of such an approach in its guidance on the European Electronic Communications Code, advocating for the use of established international standards to reduce compliance burdens on providers operating across multiple EU countries.

Ultimately, a consistent and harmonised approach to cybersecurity regulation is essential for fostering a secure and resilient digital landscape within the EU. By prioritising harmonisation, recognising established standards and focusing on tangible security outcomes, the EU can unlock the full potential of NIS2 and bolster its collective cybersecurity position.

Recommendations:

- To ensure the effective implementation of the Directive, the NIS Cooperation Group should develop further recommendations focusing on elements of the Directive that require harmonisation across Member States, similar to the recommendations already published concerning Article 28, which deals with the establishment of a database for domain name registration data.
- In addition, the European Commission could boost its direct engagement with and written guidance to Member States, providing counsel to governments starting their transposition processes to avoid unnecessary deviation, as well as intervening with Member States whose draft transposition measures deviate from the Directive.

Scope

Early transposition efforts have included different definitions for which sectors and entities would fall in scope of the Directive. The Hungarian transposition, for instance, adds some (sub)sectors to the original NIS2 sectors whilst the draft Czech Republic transposition demonstrates divergence in its definition of ‘important’ and ‘essential’ entities, potentially leading to discrepancies in which organisations fall under the scope of the regulation.

Recommendation:

- The European Commission should provide guidance to Member States on the scope of the NIS2 Directive to streamline its transposition.

Reporting

Different Member States have set divergent reporting obligations during their transposition processes. In Hungary and Croatia, for example, cybersecurity incidents must be reported ‘without delay’. There is also no explicit requirement to notify the computer security incident response team (CSIRT) or the competent authority within 24 hours of becoming aware of a ‘significant incident’ or an early warning thereof or to report the ‘significant incident’ to the CSIRT or competent authority within 72 hours of becoming aware of it.

Tha said, the current legislative landscape for cybersecurity requires many reporting obligations. Entities need to report incidents and vulnerabilities across Member States as well as to different entry points and regulatory authorities. For example, under the Network Code on Cybersecurity, entities have to report incidents to sectoral regulators in each Member State. In addition to the NIS2 Directive, overlapping reporting requirements are present in the General Data Protection Regulation (GDPR), Digital Operational Resilience Act (DORA) and Cyber Resilience Act (CRA). Especially for entities operating across borders and providing services to clients across sectors, this creates an overly complex framework that draws operational resources into administrative tasks. Member States would lack comprehensive situational awareness if the same incident were reported multiple times and to various sectoral authorities.

Recommendations:

- To avoid multiple reporting and dispersal processes, the national notification entry points under the NIS2 Directive should serve as key points of contact under other legislation that requires notifications.
- To ensure harmonisation with the CRA, the NIS2 Directive should prioritise reporting to national CSIRTs over the competent authorities. This approach would also improve trust and streamline the overall information-sharing framework.
- Confidentiality of the sensitive information shared in notifications under the NIS2 Directive, CRA, GDPR and DORA should be prioritised. Member States should work on technical requirements for the reporting channels and ensure a common high level of security in the government entities that are assigned as reporting entry points.

Risk management measures

In October, the EU published its implementing regulation on security controls and incident reporting requirements for digital infrastructure like cloud, managed and Domain Name System (DNS) services. However, none of the Member State transposition laws released so far even reference this implementing regulation (mostly due to timing). Many will ask if entities must follow Member State cybersecurity risk-management measures for cloud, managed and DNS services (like Hungary's own Hungarian audit standard or Belgium's CyFun or ISO 27001 reference) or the implementing regulation measures.

Recommendation:

- It would be useful for national transposition laws to address this point so it does not create yet another layer of needless complexity. Member State laws should clarify whether companies within the scope of the implementing regulation (eg cloud service providers and managed service providers) and which meet the security requirements of this regulation are deemed to have satisfied Member State security requirements. This would provide legal certainty and confirm that companies in scope of the implementing regulation should be guided by its requirements to comply with the NIS2 framework.

Security audit requirements

Particularly concerning are the divergent security requirements and related security audits that entities need to follow in each jurisdiction, as these are the most time-consuming and costly, with no obvious cybersecurity benefit.

For public electronic communication services, entities have to follow the NIS2 implementing laws of every EU country they offer their services in, which is all 27 Member States. This is due to the scope of the jurisdiction clause of the NIS2 Directive (Article 26), which is challenging.

In many cases, while each country requests its own audit, this audit would take place against the same set of central processes within a company, as systems are centralised for the EU (the same processes audited 27 different times). Member states should consider mutual recognition of audits to avoid undue bureaucracy, multiplication of efforts and high fees.

Due to a broad scope, the mandatory self-audit or authority audit requirements appear unduly burdensome and disproportionate for a number industries and sectors. These processes may make sense when an incident has been reported but not proactively on a periodic basis. For example, there is no logical reason for a distributor of fast-moving consumer goods such as cleaning or cosmetic products (eg face creams) – which are a 'chemical mixture' according to the Registration, Evaluation, Authorisation and Restriction of Chemicals Regulation – to be subject to a mandatory audit by a cybersecurity authority.

In Hungary, for example, companies will have to carry out periodic audits by one of four third-party auditors approved by the Hungarian government to Hungarian standards, which will be shared with the Hungarian government. In Belgium, companies will have to carry out a different audit to Belgian government-approved standards (either Belgium's CyFun standard or ISO 27001) on a periodic basis.

Although most Member States have yet to move forward their NIS2 Directive implementing laws, it is extremely burdensome for companies to be subject to a whole series of different audit requirements with different standards on a periodic basis. These multiple conflicting audit requirements are not making the EU more secure.

Recommendation:

- Member States should develop a mutual recognition policy and accept audits that are conducted in other Member States in accordance with that country's EU NIS2 transposition law or accept a pan-European audit and certification as presumption of conformity on a national level. Member State authorities would still have the option to perform additional ad-hoc assessments whenever they want as part of their general supervisory powers, but allowing reciprocity for ongoing third-party audit requirements would both ensure compliance while also streamlining the administrative burden for organisations and promoting the digital single market.

Interaction with sector-specific regulations

The application of the NIS2 Directive to regulated industries further complicates regulatory oversight. This is particularly the case for the aerospace and defence sector, where companies are subject to specific sets of rules, including on cybersecurity, overseen by the European Aviation Safety Agency (EASA). One such set of rules is the so-called 'Part-IS', a cybersecurity regulation requiring approved organisations to establish an information security management system (ISMS) and report significant cybersecurity vulnerabilities and incidents to their competent authorities. As part of the ISMS, organisations need to perform a risk assessment to identify threats and implement appropriate measures commensurate to the identified risk. Competent authorities must audit and approve the ISMS on an ongoing basis. These requirements apply to organisations of all sizes and often go even beyond the scope of the NIS2 Directive.

EASA's Part IS provides more detailed and comprehensive obligations for aerospace companies to protect against threats to aviation safety, whilst the NIS2 Directive aims to generally protect against threats to public safety and the EU economy. However, threats to the EU economy through attacks on manufacturers (eg aerospace manufacturers) are minimal due to the rate of production of aircraft and parts and nature of their operation. The resulting economic impact is below the thresholds to even justify the inclusion of aerospace manufactures as 'Important Entities' under the NIS2 Directive. A comparative analysis of Part IS with the NIS2 Directive is available here.

Moreover, given the horizonal nature of the NIS2 Directive, sector-specific rules should be closely aligned with the NIS2 framework. For any upcoming sector-specific cybersecurity rules, the NIS2 Directive should be a baseline legal framework, while more specific sectoral rules should be introduced as implementing acts.

Recommendations:

- NIS2 requirements should be limited to the applicable functions in an organisation (eg manufacturing-related systems) for critical and essential entities. This would reduce potential burdens and conflicts with other regulations. Furthermore, there is an imperative need to recognise sector-specific legislation as *lex specialis* to the NIS2 Directive. This would significantly reduce the burden between overlapping regulations, as further exemplified at the beginning of this document. Since the adoption of Part IS as *lex specialis* is allowable under Art. 4 and recognition of aviation-specific cybersecurity risk management is recommended under Recital (29) of the NIS2 Directive, Member State authorities should recognise Part IS as *lex specialis* to NIS2.
- Member States should leverage the principle laid out in Recital 22 of the NIS2 Directive. According to this provision, any future sector-specific acts should be based on the NIS2 framework and therefore be adopted as an implementing act for the NIS 2 Directive. This would ensure better harmonisation across cyber legislation and clearer rules for entities. That said, the European Commission and Member States should first assess whether there is a clear need for additional requirements, given that a comprehensive cybersecurity framework is already in place.

Conclusion

The NIS2 Directive has the potential to be a cornerstone of the EU's cybersecurity strategy, driving improved security and resilience across Member States. However, its success hinges on effective and harmonised implementation. Fragmentation in national approaches risks undermining the Directive's objectives and creating unnecessary burdens for businesses, particularly those operating across borders.

To overcome these challenges, the European Commission and Member States must prioritise consistency in transposition and align on shared standards. Efforts to streamline reporting frameworks, ensure mutual recognition of audits and respect the role of sector-specific regulations are critical. Collaboration between stakeholders, guided by a commitment to achieving tangible security outcomes, can pave the way for a robust and unified cybersecurity framework.

AmCham EU remains committed to supporting the EU in fostering a secure and competitive digital economy. By addressing these implementation challenges, the EU can not only strengthen its cybersecurity posture but also create an environment conducive to innovation, investment and growth in the digital age.