Harmonizing Cybersecurity Practices

The Requirements and Challenges of the EU NIS2 Directive

Cyberthreats constantly evolve, and new attack vectors, techniques and vulnerabilities regularly emerge. Keeping pace with the ever-changing threat landscape and ensuring regulatory compliance requires investments in technology, training and expertise. Enterprises must continually update their security measures, incident response plans and risk assessments—which require financial resources, proper technology infrastructure and cybersecurity personnel with the necessary skills—so they can address stakeholders' expectations.

To address this, the European Union adopted the NIS2 Directive. This directive highlights the importance of enhancing cybersecurity practices and protecting critical infrastructure and digital assets, including allocating adequate resources, obtaining legal and regulatory guidance, building cybersecurity expertise, and fostering a culture of compliance. It provides enterprises with incident notification requirements, reporting types, timelines and information required for compliance. Enterprises in the eurozone must understand the NIS2 Directive challenges and be proactive in complying with the incident notification requirements to enhance their cybersecurity posture and protect critical infrastructure and digital services.

NIS2 Directive's Rationale

Given the increased digitalization, greater interconnectedness of sectors, and heightened cybersecurity risk in today's world, the effectiveness of the EU Network and Information Systems Directive (EU) 2016/1148 (NIS1) is limited, resulting in fragmentation across the European Union at various levels.[1] Recognizing NIS1's limitations, the Council of the European Union adopted Directive (EU) 2022/2555 (NIS2 Directive) on 28 November 2022, after its earlier adoption by the European Parliament.[2] The NIS2 Directive expands the scope of covered entities, specifies management liabilities, and outlines how to carry out control activities and report breaches. The NIS2 Directive offers better guidance, clarity and harmonization of the cybersecurity requirements and practices across the European Union.[3] It includes new provisions and obligations related to incident response, supply chain security, encryption and vulnerability disclosure, and it imposes cyberrisk management, incident reporting and information sharing obligations on private and many public entities involved in various sectors.[4] It applies to multiple enterprises, including operators of essential services (OESs) and digital service providers (DSPs).

Significance of the NIS2 Directive

The NIS2 Directive is significant because it recognizes the importance of cybersecurity in the

ANTONIO M. VILLAMOR, JR. | CISA, CISM, CDPSE, CFE, CIA, CMA, CRMA, MBCS, MIEEE

Is the head of the internal audit unit of the International Center for Agricultural Research in the Dry Areas, a research institution dealing with international food security.

YIANNA DANIDOU | PH.D.

Is a lecturer at the European University of Cyprus (Engomi, Cyprus) and director of the CYBER.EUC Research Center.

functioning of critical infrastructure—especially the crucial role of DSPs and OESs, which must notify competent authorities of any incidents that significantly affect the continuity of their services.[5] The NIS2 Directive outlines specific requirements that DSPs and OESs (including small and microenterprises) must adhere to, such as incident reporting obligations, risk management, and technical and organizational security measures. By imposing specific cybersecurity requirements, the NIS2 Directive aims to protect the systems and users of all affected enterprises, ensure that critical infrastructure remains operational and resilient in the face of cyberthreats and cyberattacks, prevent confusion, and ensure that everyone is aware of their obligations.

The NIS2 Directive also provides a framework for EU member states to work together to combat cyberthreats and promote a culture of cybersecurity awareness and best practices. It emphasizes the importance of cooperation and information sharing among EU member states, which are essential for dealing with cyberattacks that cross borders and involve multiple actors. EU member states that work together and share information can respond more effectively to cyberincidents and prevent future attacks.

The NIS2 Directive covers a wide range of business sectors that are critical or highly critical, such as the energy, transportation, healthcare, research and financial sectors (**figure 1**).[6] Consequently, a wide variety of enterprises, from large corporations to public entities, are affected and must comply with the directive, making it a significant legal and regulatory development with far-reaching implications for the EU cybersecurity landscape. In addition, the NIS2 Directive does not preclude including small and microenterprises at high risk because it has built-in flexibility to consider them.[7]

Incident Notification Requirements, Reporting Types, Timelines and Required Information

One of the new incident notification requirements for OESs and DSPs is that they must notify the appropriate authorities of incidents within tight time limits, depending on the severity and impact of the incident. In the case of a cyberincident that significantly impacts the security of the network and information systems, OESs and DSPs must notify the competent authority designated by the member state within 72 hours of becoming aware of the incident. Notification must include specific information, such as details about the incident, the potential consequences, and the mitigating measures taken or proposed.

Enterprises must submit two types of incident reports: initial and final. The initial report must provide an overview of the incident within 72 hours of recognition. After resolving the incident, the enterprise must submit a final report, including a comprehensive analysis of root causes, impacts and lessons learned. The timeline for submitting the final report varies, ranging from 14 days for minor incidents to 90 days for major incidents. Enterprises must also provide information about the affected services, systems and networks, and any third-party providers or suppliers suspected of being involved. The NIS2 Directive further mandates that enterprises share information about known vulnerabilities and threats and any relevant technical and organizational security measures in place.

Keeping pace with the ever-changing threat landscape and ensuring compliance with the NIS2 Directive's requirements require investments in technology, training and expertise.

Challenges and Considerations

The emerging and growing cybersecurity threat landscape is the key obstacle to adhering to the NIS2 Directive. Keeping pace with the ever-changing threat landscape and ensuring compliance with the NIS2 Directive's requirements require investments in technology, training and expertise, which may be difficult for small enterprises or those who have limited resources. Enterprises must continually update their security measures, incident response plans and risk assessments, which requires financial resources, proper technology infrastructure, and cybersecurity personnel with the necessary skills. It could also require changes in business processes, technologies and organizational structures, which may necessitate internal coordination, cultural change, and implementation of recent technologies or security measures.

LOOKING FOR MORE?

- Read *Reporting Cybersecurity Risk to the Board of Directors. https://www.isaca.org/reporting-cyberrisk-to-bod*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 1

Highly Critical Sectors

Highly Critical Sectors	Examples
Energy (e.g., electricity, district heating and cooling, oil, gas, hydrogen)	Market participants providing aggregation, demand response or energy storage services; operators of recharging points providing recharging to end users; distribution system operators; and transmission system operators and producers
Transport (e.g., air, rail, water, road)	Air carriers; airport managing bodies and entities operating ancillary installations within airports; traffic management control operators providing air traffic control; railway operators of service facilities; infrastructure managers; inland, sea and coastal passenger and freight water transport enterprises; managing bodies of ports and entities operating works within ports; operators of vessel traffic services; road authorities who handle traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a nonessential part of the general activity; and operators of intelligent transport systems
Banking	Credit institutions
Financial market infrastructure	Operators of trading venues and central counterparties
Healthcare	Healthcare providers, EU reference laboratories, entities conducting research and development activities related to medicinal products, entities manufacturing basic pharmaceutical products and conducting pharmaceutical operations, and entities manufacturing medical devices critical during a public health emergency (public health emergency critical devices list)
Drinking water	Suppliers and distributors of water intended for human consumption, excluding those for which distribution of water for human consumption is a nonessential part of the general distribution of other commodities and goods
Wastewater	Entities collecting, disposing of or treating urban wastewater, domestic wastewater or industrial wastewater, excluding those for which these activities are a nonessential part of the general activity
Digital infrastructure	Internet exchange point providers; domain name service (DNS) providers, excluding operators of root name services; top-level domain (TLD) name registers; cloud computing service providers; data center service providers; trust service providers; providers of public electronic communication networks; and providers of publicly available electronic communication services
Information and communications technology (ICT) service management (business-to-business)	Managed service providers and managed security service providers
Public administration	Public administration entities of central governments and regional levels
Space	Operators of ground-based infrastructure owned, managed and operated by EU member states or private entities that support space-based services, excluding providers of public electronic communication networks
Other Critical Sectors	**Examples**
Postal and courier services	Postal service providers, including providers of courier services
Waste management	Entities conducting waste management, excluding those for which waste management is not the principal economic activity
Manufacture, production and distribution of chemicals	Entities manufacturing and distributing substances or mixtures and those producing articles from substances or mixtures
Production, processing and distribution of food	Food businesses engaged in wholesale distribution and industrial production and processing
Manufacturing of medical devices and in vitro diagnostic medical services; computer, electronic and optical products; machinery and equipment; motor vehicles, trailers and semitrailers; and other transport equipment	Entities conducting any economic activities referred to in section C, divisions 26–30, of Statistical Classification of Economic Activities in the European Community (NACE) Rev. 2[a]
Digital providers	Providers of online marketplaces, online search engines and social networking services platforms
Research	Research organizations

Source: a) Eurostat, *NACE Rev. 2: Statistical Classification of Economic Activities in the European Community*, Luxembourg, 2008, *https://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF*

Enterprises may find it difficult to determine the severity of incidents and classify them correctly to meet the directive's reporting timelines and other requirements.

The requirements of the directive may be complex and challenging to implement and may require considerable time, effort and resources, including cybersecurity, legal and regulatory expertise. Enterprises may face resource constraints that hinder their ability to implement the NIS2 Directive,[8] including budget limitations, lack of skilled cybersecurity personnel and inadequate technology infrastructure. In addition, enterprises may need to navigate complex legal and regulatory frameworks at the national and EU levels involving specific industry sectors, geographic regions and legal environments. The NIS2 Directive also requires interactions with multiple stakeholders, including regulatory authorities, industry regulators and law enforcement agencies. Managing these interactions, coordinating incident notifications, and ensuring compliance with varying requirements can be challenging, particularly for enterprises operating under several different authorities.

Noncompliance with the NIS2 Directive can have profound consequences, including fines, penalties and reputational damage. Devoting the significant effort and resources required to address these new requirements may be difficult, but EU member states must establish effective, proportionate and dissuasive sanctions for noncompliance. Enterprises that cannot comply with the incident notification requirements may face financial penalties of up to EU€10 million or 2 percent of worldwide annual turnover, whichever is higher. Repeat or serious noncompliance may lead to fines of up to EU€20 million or 4 percent of worldwide annual turnover, whichever is higher.

Complying with the incident notification requirements of the NIS2 Directive may also pose challenges for OESs and DSPs, including the need for effective incident response plans, and communication protocols to ensure the timely and accurate reporting of incidents. Enterprises may find it difficult to determine the severity of incidents and classify them correctly to meet the directive's reporting timelines and other requirements.

The NIS2 Directive mandates that enterprises share sensitive information about incidents and security measures with relevant authorities, which may raise concerns about data privacy, confidentiality and potential legal liability. Enterprises must navigate data privacy considerations, such as compliance with the EU General Data Protection Regulation (GDPR), when sharing incident-related information, which can complicate compliance efforts.

The NIS2 Directive has an extraterritorial reach and applies to various sectors, including OESs and DSPs. Even non-EU enterprises may be subject to its requirements if they provide services to EU-based enterprises or citizens.[9] Like the GDPR, the NIS2 Directive is important for enterprises operating outside the European Union that deal with enterprises within the European Union or that provide services to EU citizens. For example, the directive has important implications for enterprises operating in the ecommerce and digital marketing sectors, where cross-border transactions are common. These enterprises must comply with the requirements of the NIS2 Directive, even if they are not physically located within the European Union. OESs, DSPs and other enterprises inside and outside the European Union may have diverse levels of cybersecurity maturity, varying sizes and different operational complexities, making it difficult to achieve consistent compliance across such a diverse organizational landscape.

Best Practices for Incident Notification and Compliance

Enterprises need robust incident response processes and protocols to ensure quick incident responses and adherence to notification timelines. However, they must take proactive measures to address these issues, including allocating adequate resources, obtaining legal and regulatory guidance, building cybersecurity expertise, and fostering an organizational culture of compliance.

Despite the NIS2 Directive's novelty, enterprises can still rely on existing incident notification and compliance practices. Foremost are proper technical and organizational security measures to prevent, detect and proactively and regularly respond to cybersecurity incidents. These technical measures may include firewalls, intrusion detection and prevention systems, security information and event management (SIEM) systems, security monitoring

tools, threat intelligence, and security analytics that can identify and respond to cybersecurity incidents in real time. Organizational measures include fostering a culture of cybersecurity awareness among all employees, from top management to frontline staff, by promoting cybersecurity best practices, providing ongoing training and education on cybersecurity risk and incident reporting requirements, instituting employee awareness and training programs, and encouraging employees to report any potential incidents they encounter. Another good approach is assigning legal or compliance staff members to regularly review relevant legislation, guidance documents and industry best practices and to incorporate any necessary changes into incident response plans and procedures. Enterprises must also have strong vendor management practices, including conducting due diligence on vendors' cybersecurity practices and incident reporting capabilities and reviewing contracts to ensure that they require early notification of any cybersecurity incidents that may affect the vendors' services.

An effective incident response and escalation plan should outline the roles and responsibilities of the incident response, management, legal and communication teams and the procedures for detecting, responding to and reporting cybersecurity incidents. This plan should be reviewed, updated and periodically evaluated to ensure its effectiveness, especially during enterprise IT environment changes. Performing simulated incident response drills can identify gaps or weaknesses in the incident response plan that could be devastating in the event of an incident.

This plan should also contain clear communication protocols to ensure that DSPs, OESs and other enterprises report incidents accurately and promptly to the competent authority. It must include designated points of contact, communication channels and escalation procedures to ensure that incident reports reach the proper authority within the allotted time.

Enterprises should provide staff with regular training and education on the criteria for determining the severity of incidents, the information they must include in incident reports, and the timelines for reporting. Staff members should be able to identify and report incidents promptly and accurately, and to comprehensively analyze cybersecurity incidents, including root causes, impacts and lessons learned. In addition, enterprises should maintain accurate and up-to-date documentation and records of all incidents, including initial and final reports, and any relevant technical and organizational security measures in place. These records can indicate compliance with the NIS2 Directive and demonstrate an effort to comply with incident notification requirements. Equally important, enterprises should stay updated on the latest regulations and guidelines related to incident notification, including any updates or amendments to the NIS2 Directive.

Organizations should conduct thorough postincident analyses to identify incident response processes in need of improvement. They should incorporate lessons learned into updated incident response plans and procedures. Likewise, OESs and DSPs should conduct regular penetration testing and vulnerability assessments to identify and address any system and network vulnerabilities or weaknesses.

Conclusion

The NIS2 Directive is a legal instrument that guides the improvement of cybersecurity practices in the European Union. It sets specific cybersecurity requirements for DSPs, OESs and other enterprises that are vital in ensuring systems' and users' continuity, safety and security. It serves as a framework for establishing comprehensive and consistent cybersecurity practices across the region, aiming to prevent and combat cyberthreats and cyberattacks and promote a culture of cybersecurity awareness and best practices.

DSPs, OESs and other enterprises must recognize the importance of complying with the NIS2 Directive. Compliance with its incident notification requirements is crucial to avoid severe consequences such as economic loss, reputational damage and legal liability. Enterprises must establish robust incident response plans, foster cybersecurity awareness and implement effective communication protocols. Regular drills and simulations, continuous monitoring and detection of incidents, clear incident escalation processes, and thorough postincident analysis and improvement are essential steps toward compliance. In addition, it is important to regularly review and update incident response plans to align with emerging threats and best practices.

Compliance with the NIS2 Directive will help DSPs, OESs and other enterprises improve their cybersecurity measures and reduce the risk of cyberthreats and cyberattacks by enhancing their cybersecurity postures and protecting their critical infrastructure and digital services. Taking proactive steps to manage cybersecurity incidents and protect digital assets effectively ensures resilience in the face of growing cyberthreats. Organizations should consider an ongoing process that requires continuous attention and adaptation. However, implementing the NIS2 Directive may present challenges, such as allocating adequate resources, obtaining legal and regulatory guidance, building cybersecurity expertise, and fostering a culture of compliance. The NIS2 Directive is crucial for enhancing cybersecurity practices in the European Union and globally, and compliance with its incident notification requirements can better safeguard critical infrastructure and digital assets, contributing to a safer digital environment for everyone.

The NIS2 Directive is crucial for enhancing cybersecurity practices in the European Union and globally, and compliance with its incident notification requirements can better safeguard critical infrastructure and digital assets.

Endnotes

1 Chatain, B.; "Cybersecurity: Parliament Adopts New Law to Strengthen EU-Wide Resilience," European Parliament News, 11 October 2022, *https://www.europarl.europa.eu/news/en/press-room/20221107IPR49608/cybersecurity-parliament-adopts-new-law-to-strengthen-eu-wide-resilience*

2 Persoff, S.; S. Phillips; H. Ovaisi; R. Flakoli; *NIS2 Directive: Europe Revamps Its Cybersecurity Framework,* Clifford Chance, United Kingdom, November 2022, *https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/11/nis-2-directive-europe-revamps-its-cybersecurity-framework.pdf*

3 Wulff, F. G. H.; "NIS2.0—EU's New Network and Information Security Directive (Explained)," Tricent Blog, 12 December 2022, *https://www.tricent.com/blog/nis2*

4 International Association of Privacy Professionals (IAPP), "European Parliament Approves NIS2 Directive," IAPP Daily Dashboard, 10 November 2022, *https://iapp.org/news/a/european-parliament-approves-nis2-directive/*

5 Enterprise Defense, "NIS2: How Will It Impact Your Organisation?" 2 February 2022, *https://enterprisedefence.com/blog/nis2/*

6 The European Parliament and the Council of the European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council, 14 December 2022, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN*

7 Barina, E.; "NIS2 Directive: How Will It Affect Companies?" *Blaze*, 6 March 2023, *https://www.blazeinfosec.com/post/nis-2-directive/*

8 Nicaise, V.; "NIS2 Directive: What's Changing?" Stormshield, 26 September 2022, *https://www.stormshield.com/news/eu-nis2-directive-whats-changing*

9 Vladimirova-Kryukova, A.; "The Influence of the NIS2 Directive in and Outside of the EU," ISACA Now, 10 November 2021, *https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/the-influence-of-the-nis2-directive-in-and-outside-of-the-eu*