HADRIAN

Securing Tomorrow:
A Guide to NIS2 Compliance

Table of Contents

Urgency, Significance & Consequences

The Network and Information Systems (NIS2) Directive, a key European Union legislation, stands as a crucial step towards fortifying cybersecurity and bolstering the resilience of critical infrastructure across the EU. Originating from the original NIS directive introduced in 2016, the NIS2 directive signifies an updated and expanded approach, extending its coverage to include digital service providers, thus broadening its scope.

Covering an extensive range of sectors, including energy, transport, banking, healthcare, water supply, and digital infrastructure, the NIS2 directive mandates that organizations providing essential services or relying on network and information systems adhere to heightened cybersecurity measures. The directive's importance lies in its mission to enhance the EU's collective resilience against cyber threats, recognizing the potential for devastating consequences, from economic damage to jeopardizing lives, in the face of cyber-attacks on essential services.

Acting swiftly is imperative for organizations, considering the evolving landscape of cyber threats. The NIS2 directive not only updates and expands its predecessor's framework but also imposes stricter and more consistent penalties for non-compliance. Failure to adhere to the directive's provisions can lead to severe consequences, including substantial fines and potential legal repercussions.

The quick answer:

The NIS2 Directive underscores the urgency for organizations to fortify their cybersecurity posture promptly. It is a pivotal tool in addressing contemporary cyber threats, promoting collaboration among EU member states, and establishing a harmonized framework for incident reporting. Organizations must act now to ensure compliance, mitigate risks, and contribute to the collective resilience of the European Union against cyber threats.

NIS Evolution: From Pioneering NIS to Empowering NIS2

In the cybersecurity landscape, the EU took a historic step with the introduction of the Directive on security of network and information systems (NIS Directive) in 2016. Simultaneously, the EU introduced the General Data Privacy Regulation (GDPR). Due to its wider scope, specific requirements, and more significant penalties, the NIS directive was largely eclipsed by the GDPR. However, both marked the EU's maiden venture into legislating cybersecurity, aimed at establishing a high common standard across all member states.

Adopted on July 6th, 2016, the NIS Directive targeted operators of essential services and digital service providers (DSPs). Essential services encompassed sectors vital to society, including energy, transport, banking, health, and more. Originally, 7 services were defined as essential, but this is now changing with the implementation of NIS2. Meanwhile, DSPs, such as cloud service providers, online marketplaces, and search engines, were recognized for their digital impact.

NIS Evolution: From Pioneering NIS to Empowering NIS2 (Cont.)

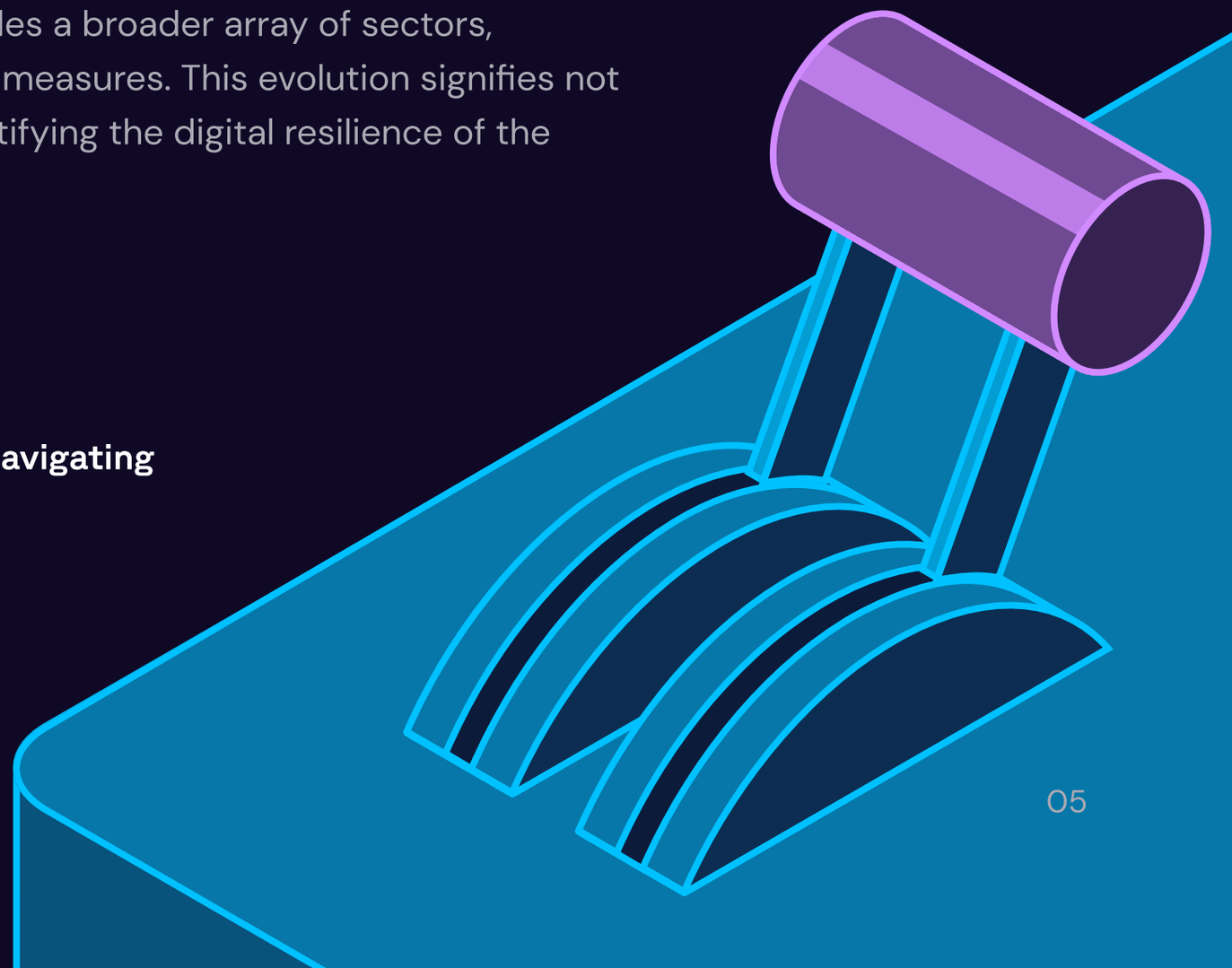
Fast forward to 2020, and the proposal of the Directive (EU) 2022/2555, known as NIS2, marked a significant evolution from its predecessor. NIS2 brings notable improvements to EU cybersecurity, introducing a cyber crisis management structure (CyCLONe), heightened harmonization of security requirements, and extended coverage to new areas like supply chain, vulnerability management, core internet, and cyber hygiene.

NIS2 fosters collaboration and knowledge-sharing among member states through innovative approaches like peer reviews. Its expanded scope includes a broader array of sectors, compelling more entities to adopt robust cybersecurity measures. This evolution signifies not just a legal transition but a strategic enhancement in fortifying the digital resilience of the European Union against evolving cyber threats.

Empowering EU Organizations: Navigating the Digital Security Landscape

2 minute read

Read blog post



The Evolution: Key Differences Between NIS and NIS2

Expanded Applicability

NIS2 broadens its reach, encompassing essential and major organizations.

Medium and large enterprises, alongside potential designations for smaller high-risk companies, now fall under compliance obligations.

Unified Company Classification

The NIS2 directive replaces the distinction between operators of essential services and digital service providers.

All companies are categorized into essential and important sectors, streamlining regulatory clarity.

Supply Chain Security Focus

NIS2 mandates companies to address security risks within their supply chain.

Comprehensive consideration of risks stemming from supplier relationships is a key enhancement.

Stronger Supervision & Enforcement

National authorities gain enhanced supervisory powers under NIS2.

A uniform penalty regime and reporting requirements ensure consistency across all member states.

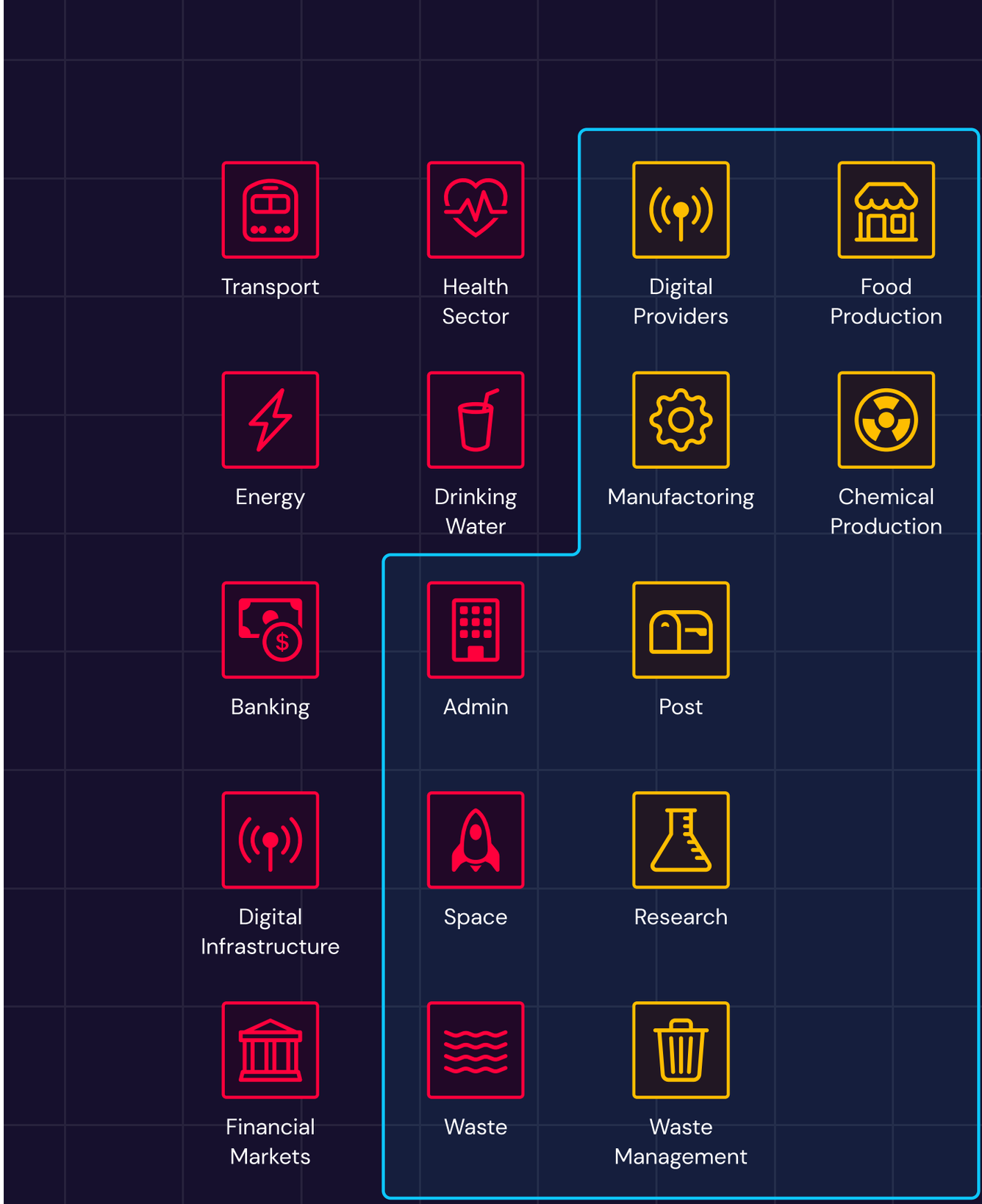
Concrete Security Standards

NIS2 introduces a list of minimum basic security standards, providing a more tangible requirements.

Scope expansion new sectors & entities

The NIS2 Directive introduces a new classification of targeted organizations: essential entities and important entities. Essential entities, subject to continuous supervision, include sectors such as energy, transportation, banking and healthcare, facing potential fines of up to €10 million or 2% of global turnover.

Important entities, with ex-post supervision, encompass sectors like waste management and digital providers, with fines up to €7 million or 1.4% of global turnover. Compliance requirements are the same for both, but essential entities bear a higher operational burden due to constant oversight.



DORA vs. NIS2: The Dual Regulations in EU Cybersecurity

The EU's financial industry faces dual regulations with NIS2 and DORA. While both enhance resilience, harmonization is crucial. Differences include responsibilities, penalties, and testing, emphasizing unique objectives. Consolidating responsibilities and harmonizing audits is key for efficiency and cost-effectiveness.

DORA: Digital Operational Resilience Act	**NIS2: Network and Information Security 2**
The Digital Operational Resilience Act, is a direct European law set to impact member states from 2025. With a focus on operational stability in the financial sector, DORA aims to fortify the industry against cyber threats, ensuring financial services remain accessible even in the face of cyberattacks.	NIS2, the Network and Information Security 2 directive, harmonizes cybersecurity requirements for the EU's basic services and vital infrastructure. Set to be transposed into national law by October 2024, NIS2 aims to enhance cybersecurity capabilities, introduce penalties, and establish reporting channels across the EU.
Key Objectives:	**Key Objectives:**
DORA's primary objective is to strengthen the digital operational resilience of the financial sector. It emphasizes the sector's ability to endure and operate despite cyber threats, prioritizing the availability and integrity of financial services.	NIS2's overarching goal is to harmonize the global level of cybersecurity across the EU. It targets essential companies and organizations, ensuring they attain a high level of digital security to safeguard critical services.

DORA vs. NIS2 (Cont.)

Regulatory Approach:	**Regulatory Approach:**
DORA introduces a directly applicable European law, signifying its universal impact across member states. In contrast to NIS2, DORA leaves the determination of penalties to national authorities, offering flexibility in enforcement.	As a directive, NIS2 requires member states to transpose its provisions into national law. However, potential variations in implementation can create challenges for multinational companies, leading to an uneven competitive landscape among EU countries.
Testing and Security Measures:	**Testing and Security Measures:**
DORA places a strong emphasis on security testing, requiring a resilience testing program at least once a year and a threat-led penetration test at least every three years. This stringent testing regimen aims to ensure the robustness of financial entities against evolving threats.	NIS2 mandates a security audit at least once every two years in Germany, with a broader emphasis on cybersecurity capabilities. While not as specific as DORA in testing requirements, NIS2 prioritizes a comprehensive approach to cybersecurity measures.
Responsibilities:	**Responsibilities:**
DORA places a strong emphasis on security testing, requiring a resilience testing program at least once a year and a threat-led penetration test at least every three years. This stringent testing regimen aims to ensure the robustness of financial entities against evolving threats.	NIS2 mandates a security audit at least once every two years in Germany, with a broader emphasis on cybersecurity capabilities. While not as specific as DORA in testing requirements, NIS2 prioritizes a comprehensive approach to cybersecurity measures.

DORA and NIS2: Which One Has Priority?

Lex Specialis Principle: DORA is the "lex specialis" of NIS2 for the financial sector. According to DORA's Recital 16, if your organization is bound by DORA, it takes precedence over NIS2.

Entities Covered by DORA: DORA applies primarily to 21 types of entities within the financial sector. If your organization doesn't fall into these categories, DORA doesn't apply to you. However, under Article 31, any critical suppliers of critical ICT services, which could include digital service/infrastructure providers under NIS2, may also be subject to DORA regulations.

- **Distinct Objectives:** NIS2 aims at enhancing the overall EU cybersecurity level, while DORA focuses on ensuring the integrity and availability of the financial sector.
- **Regulatory Status:** NIS2 is a directive, requiring transposition into national law by October 2024. DORA is a regulation, directly applicable in all EU countries from January 17, 2025.
- **Precedence and Applicability:** For entities under DORA, it prevails over NIS2. However, entities affected by both texts must still comply with NIS2 obligations, as the two serve distinct purposes.

What is a "lex specialis"?

The *lex specialis* doctrine, also referred to as generalia specialibus non derogant ("the general does not derogate from the specific"), states that if two laws govern the same factual situation, a law governing a specific subject matter (lex specialis) overrides a law governing only general matters (lex generalis).

Why is the Digital Operational Resilience Act a game-changer?

2 minute read

Read blog post

Impact for Key Stakeholders

CISOs and CTOs: Steering Cybersecurity Evolution

The NIS2 Directive brings profound changes for Chief Information Security Officers (CISOs) and Chief Technology Officers (CTOs). Stringent security obligations, including a 72-hour incident reporting window, require CISOs to ensure seamless communication with designated competent authorities like ANSSI, BSI, and CCB. Simultaneously, CTOs must oversee the development of technology solutions aligning with the updated cybersecurity landscape.

CEOs and Board Members: Navigating Regulatory Waters

For CEOs, the NIS2 Directive necessitates a keen focus on the seven specified elements, encompassing risk analysis, information system security policies, incident handling, business continuity, crisis management, and supply chain security. Collaborating closely with CISOs, CTOs, and senior executives, CEOs must devise and execute strategies ensuring compliance. Board members shoulder the responsibility of maintaining a high level of awareness, aligning cybersecurity policies with the directive, and actively overseeing compliance efforts.

SMEs: Navigating Compliance Challenges

Small to Medium Enterprises (SMEs), vital economic contributors, confront unique challenges under the NIS2 Directive. As it introduces cybersecurity obligations across critical sectors, all 27 EU Member States are mandated to incorporate these into national laws by September 2024. The resource and expertise constraints of SMEs make compliance a challenging and costly endeavor. To navigate these complexities, SMEs must engage with Managed Service Providers (MSPs), seeking guidance and implementing effective solutions for regulatory adherence.

Preparing for NIS 2 Compliance: A 5 Point Strategic Blueprint

Thorough Vulnerability Management Assessment

In anticipation of the impending NIS 2 Directive, organizations should conduct a comprehensive assessment of their vulnerability management plan. Recognizing that the status quo may no longer suffice, recalibrating penetration testing and adopting a more robust risk-based vulnerability management strategy is imperative.

Enhanced Cybersecurity Measures

In anticipation of the impending NIS 2 Directive, organizations should conduct a comprehensive assessment of their vulnerability management plan. Recognizing that the status quo may no longer suffice, recalibrating penetration testing and adopting a more robust risk-based vulnerability management strategy is imperative.

Fostering a Cybersecurity-Aware Culture

In anticipation of the impending NIS 2 Directive, organizations should conduct a comprehensive assessment of their vulnerability management plan. Recognizing that the status quo may no longer suffice, recalibrating penetration testing and adopting a more robust risk-based vulnerability management strategy is imperative.

Preparing for NIS2 Compliance: A Strategic Blueprint (Cont.)

Competent Incident Response Management

Enterprises need to develop a competent incident response management plan to ensure the adept handling of breach incidents. A comprehensive understanding of all organizational assets and a commitment to keeping them secure is paramount. This involves conducting thorough risk analyses and optimizing incident response procedures to align with NIS 2 compliance requirements.

Proactive Measures for NIS 2 Compliance

In conclusion, preparing for NIS 2 compliance demands proactive measures, strategic planning, and a commitment to elevating cybersecurity practices. CIOs and CISOs play a pivotal role in orchestrating this preparedness, safeguarding critical assets, and steering their organizations towards enhanced cybersecurity resilience.

Compliance Imperatives

Raise Organizational Awareness

Communicate legislative changes effectively to the CEO and leadership team.

Ensure a collective understanding of the compliance landscape across the organization.

Update Crisis Response Structure

Define clear roles and responsibilities in the organizational crisis response structure.

Ensure alignment with the NIS2 requirements for effective response and recovery.

Leverage Innovative Technologies

Integrate AI and other innovative technologies for efficient incident detection and prevention.

Build technological capabilities to process information, enhance operational response, and conduct forensics.

Enhance Coordination

Break down IT and business silos to foster internal cooperation.

Facilitate collaboration for external oversight, peer reviews, and incident response.

Assess and Address Internal Risks

Identify gaps in HR, legal, internal audit, supply chain, and IT practices.

Understand the impact of new legislation on current organizational practices.

Prioritize Organizational Focus

Address top priorities with the greatest financial, reputational, and operational impacts.

Update recovery and response playbooks to align with NIS2 compliance objectives.

Crafting a Strategic Roadmap

CIOs and senior leaders should implement a phased approach, considering a 30-, 90-, and 120-day roadmap. Prioritizing resources and managing risks are crucial components of achieving NIS2 compliance by the October 2024 deadline.

Actionable Steps:

Within 30 Days:

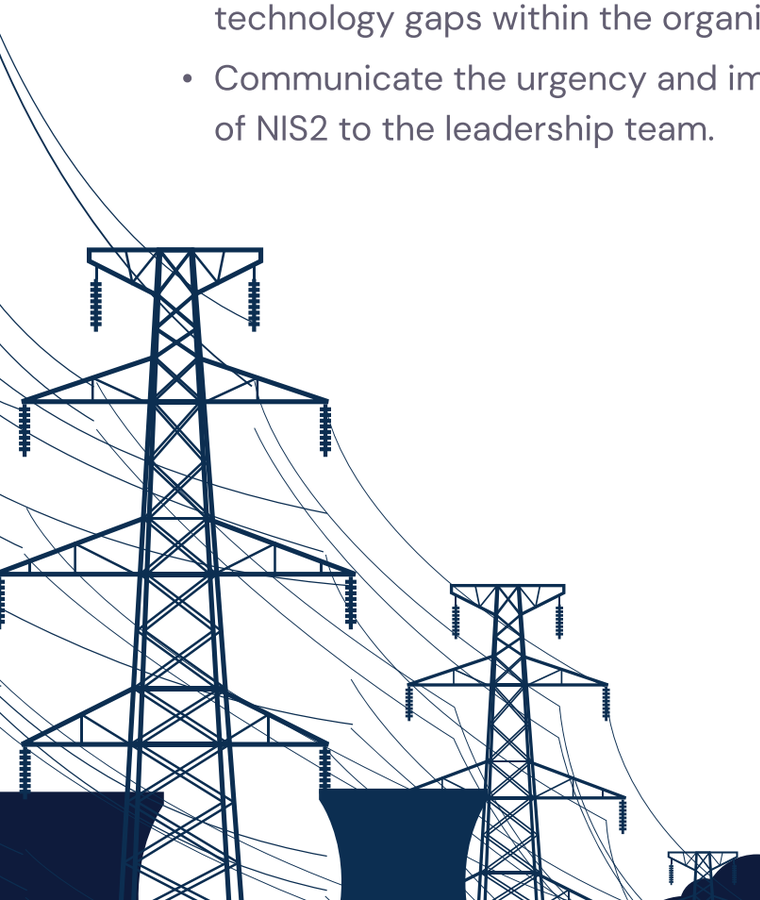
- Initiate internal risk assessments across key organizational functions.
- Identify personnel, process and technology gaps within the organization
- Communicate the urgency and impact of NIS2 to the leadership team.

Within 90 Days:

- Establish cross functional stakeholder meetings to break IT and business silos for improved internal cooperation.
- Update crisis response structure with clear roles and responsibilities.
- Compile a technology roadmap and vendor selection plan.

Within 150 Days:

- Review organizational policies and update recovery playbooks accordingly.
- Integrate AI and innovative technologies for enhanced threat detection and incident response.
- Test the organization's ability to meet reporting requirements with the regional CSIRT.



Note

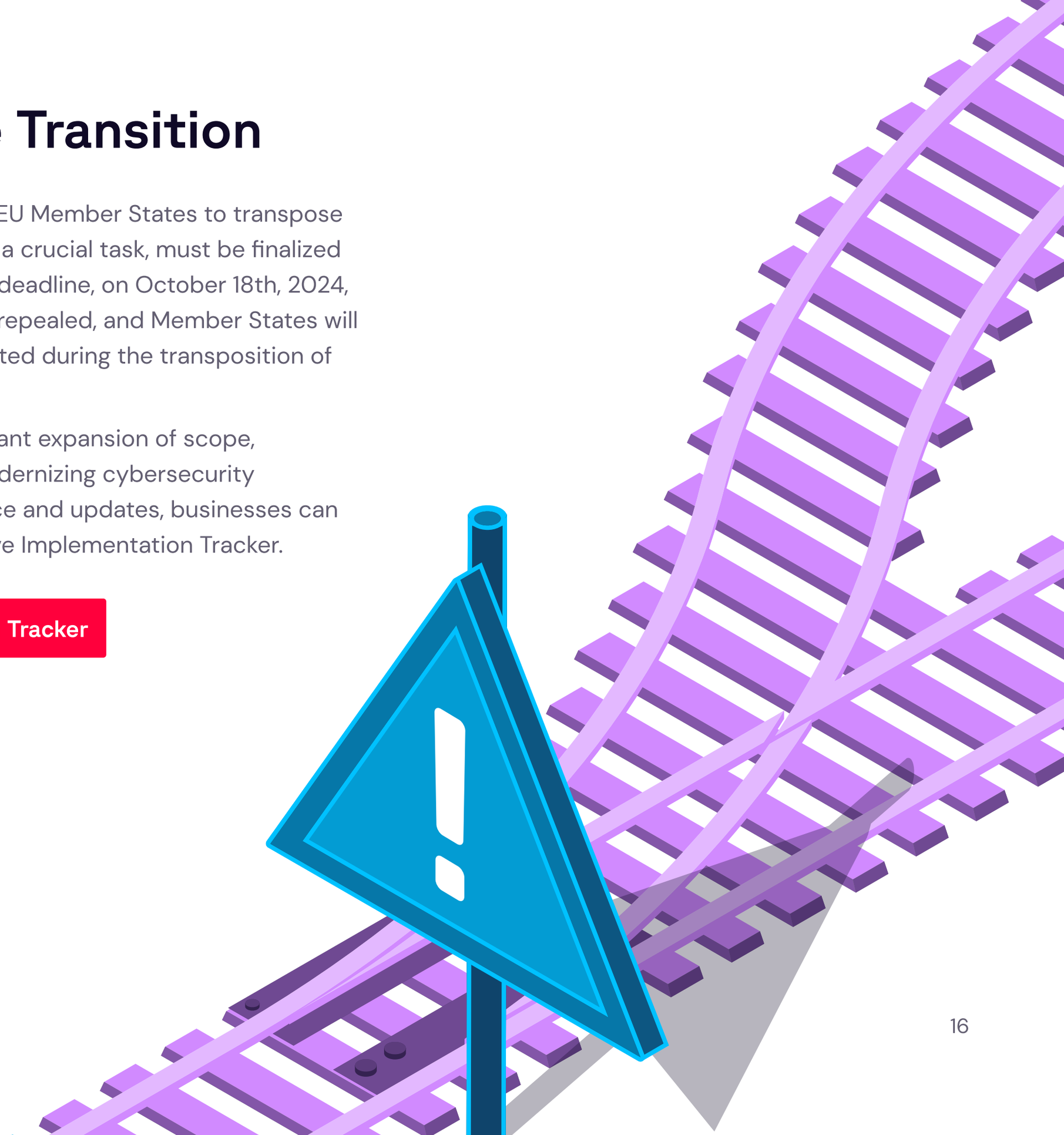
This roadmap ensures a structured and timely response, aligning your organization with the evolving cybersecurity landscape defined by the NIS2 Directive.

NIS2 Directive Transition

The NIS2 Directive necessitates EU Member States to transpose it into national law. This process, a crucial task, must be finalized by October 17th, 2024. Post this deadline, on October 18th, 2024, the existing NIS Directive will be repealed, and Member States will enforce the measures implemented during the transposition of the NIS2 Directive.

This transition signifies a significant expansion of scope, introducing new sectors and modernizing cybersecurity frameworks. For ongoing guidance and updates, businesses can rely on Bird & Bird's NIS2 Directive Implementation Tracker.

NIS2 Directive Implementation Tracker



Fines and Implications

The NIS2 Directive defines distinct consequences for non-compliance. These consequences are applicable to essential and important entities in cases of infractions such as non-compliance with security requirements or failure to report incidents.

While the exact fines may differ by Member State, the Directive outlines a minimum set of administrative sanctions for breaches of cybersecurity risk management and reporting obligations.

Administrative Fines

The directive distinguishes between essential and important entities for administrative fines. For **essential entities**, Member States are mandated to set a maximum fine threshold of at least €10,000,000 or 2% of the global annual revenue, whichever is greater. For **important entities**, NIS2 instructs Member States to impose fines with a maximum threshold of at least €7,000,000 or 1.4% of the global annual revenue, whichever is higher.

Non-Financial Consequences

Under NIS2, national supervisory authorities have the power to implement non-financial remedies, which may include:

- Compliance orders
- Binding instructions
- Mandates for security audit implementation
- Orders for notifying entities' customers about potential threats.

Criminal Sanctions Applicable to Management

NIS2 introduces provisions holding top management personally accountable for gross negligence during a security incident, Member State authorities can personally implicate organization managers in cases of proven gross negligence. This entails:

- Mandating organizations to publicly disclose compliance breaches.
- Releasing public statements that identify the individuals responsible for the violation and detailing its nature.
- For essential entities, a temporary ban on individuals holding management positions in the event of recurrent violations.
- These provisions aim to establish accountability among C-level management and deter gross negligence in the handling of cyber risks.

These measures are designed to hold C-level management accountable and to prevent gross negligence in the management of cyber risks.

How Hadrian can help you comply with NIS2?

NIS2 will require better penetration testing and risk-based vulnerability management, attack surface management, automated penetration testing, vulnerability management and exposure management.

The good news is, Hadrian can help with all of this, and more. We can help you:

Know your attack surface

NIS2 mandates effective measures to secure network and information systems. Hadrian aids compliance by providing continuous asset discovery, ensuring visibility and mitigating risks from poorly managed assets. Our services extend to protecting IoT and OT assets, identifying attack vectors, and comprehensive cloud monitoring to prevent breaches.

Manage vulnerabilities

Managing external attack surfaces is increasingly intricate as assets are interconnected. Hadrian simplifies cybersecurity with automated penetration testing, simulating hacker techniques through event-based AI for thorough security validation. Our real-time vulnerability management solution identifies and addresses critical vulnerabilities, fortifying your defense against potential threats.

Protect the supply chain

Hadrian can defend against supply chain attacks with 3rd party risk monitoring. We continuously assess 3rd party applications for risks that could result in a breach of your critical data.

About Hadrian

Defensive security should be validated by offensive security. Hadrian provides the hacker perspective, revealing the targets and methods that could be used in a real-world data breach. Hadrian's continuous and comprehensive testing discovers and validates risks completely autonomously.

Hadrian's platform combines attack surface discovery, automated penetration testing, and threat exposure management technologies in a cloud-based and agentless platform. The cutting-edge technology is constantly updated and improved by Hadrian's in-house hacker team.

> ‘What's exciting about what Hadrian is doing is they solved a seemingly impossible puzzle: finding weaknesses in a complex network with human-like detail, at scale, from the outside and continuously. What usually takes a dedicated team of security engineers a few weeks to figure out for one system, they can do in minutes for thousands of systems.’
>
> **Tiago Teles - Security Lead, ABN AMRO**

Trusted by

ABN·AMRO · SHV ENERGY · macmillan education · CTC GLOBAL

WeatherTech · LEROY MERLIN · LOTTOMATICA · CA

RITUALS... · BIOLANDES · nedap · Van Oord

NIS2 Impact Per Industry

NIS2: Energy

Sector Overview:

Encompasses electricity, oil, gas, district heating, and hydrogen. Contributes €250B annually to the European economy, employing 1.6 million people.

Critical Infrastructure Status:

Energy sector's vital role deems it highly susceptible to NIS2. Imposes specific cybersecurity requirements to safeguard critical infrastructure.

Data Protection and Privacy:

Mandates protection of personal data processed by energy companies. Requires reporting incidents impacting data security and grants consumers rights to information and deletion.

Compliance and Enforcement:

Companies appoint a responsible person for NIS2 compliance oversight. Regular risk assessments and cooperation with national competent authorities are essential.

More information

NIS2 Implications:

- Aims to enhance security and resilience against cyber threats.
- Requires technical and organizational measures for incident prevention, detection, and response.

Cybersecurity Challenges:

- Supply chain risks, APTs, aging technology, ICS vulnerabilities, and interconnected systems pose threats.
- Control system security vulnerabilities susceptible to ransomware attacks.

Market Impact:

- NIS2 fosters consumer confidence, increasing competition and market growth.
- Promotes a sustainable and responsible energy sector by safeguarding personal data.

NIS2: Chemical

Sector Overview:

One of Europe's largest manufacturing sectors, contributing €45B annually to the economy. Employs over 1.2 million people, supporting diverse chemical productions.

Critical Infrastructure Status:

Chemical sector, vital for innovation and industrial competitiveness, is critical infrastructure. Categorized as an "important entity" under NIS2 due to its role in construction, agriculture, transportation, and energy.

Impact on Supply Chains:

NIS2 necessitates rigorous risk assessments and security measures for supply chains. Increased oversight and auditing of supply chain security to meet stringent cybersecurity requirements.

Compliance and Enforcement:

High regulatory standards and compliance costs pose challenges. Smaller companies may face a competitive disadvantage.

More information

NIS2 Implications:

- Emphasis on improved supply chain security for chemical manufacturers.
- High compliance costs may pose challenges, especially for smaller companies.
- Broad impact on interconnected supply chains, necessitating additional administrative efforts.

Cybersecurity Challenges:

- APTs, attacks on industrial control systems, cloud service security risks, supply chain vulnerabilities, DDoS attacks, and malware threats pose significant challenges.
- Industry's critical nature makes it a prime target for cyberattacks.

Market Impact:

- NIS2 directive expected to drive significant changes in the chemical sector.
- Investments in new technologies may lead to increased collaboration, information sharing, and improved cybersecurity.

NIS2: Infrastructure

Sector Overview:

Encompasses telecom, DNS, TLD, data centers, trust services, and cloud services. Projected annual revenue of €85.4B in the EU digital infrastructure market, with 1335 colocation data centers in Europe.

Essential Entity Recognition:

Digital infrastructure, crucial for modern society, recognized as essential entities under NIS2. Acknowledges the sector's significance in supporting the modern economy.

Security Upgrades:

NIS2 mandates enhancements to physical security measures, requiring installations like security cameras. Acknowledges the risk posed by physical security threats to organizations in the digital infrastructure sector.

Incident Response Planning:

Organizations must develop robust incident response and recovery plans. Identification of response leaders, rapid information sharing, and evidence-gathering procedures are crucial.

Regulatory Oversight:

Anticipated increase in regulatory oversight as EU authorities enforce NIS2 requirements. Companies held accountable for safeguarding critical systems and networks.

More information

NIS2 Implications:

- Focus on upgrading physical security measures to counter evolving threats.
- Emphasis on incident response and recovery planning for effective cybersecurity measures.
- Anticipated heightened regulatory oversight to ensure compliance.

Cybersecurity Challenges:

- Ransomware threats, shortage of cybersecurity professionals, third-party vendor risks, physical security concerns, IoT vulnerabilities, and compliance complexities.
- Diverse challenges make the sector a high-value target for malicious actors.

Market Impact:

- NIS2 expected to drive demand for innovative cybersecurity solutions.
- Encourages competition and innovation in the digital infrastructure sector, fostering a level playing field.

NIS2: Digital Infrastructure

Sector Overview:

Encompasses telecom, DNS, TLD, data centers, trust services, and cloud services. Projected annual revenue of €85.4B in the EU digital infrastructure market, with 1335 colocation data centers in Europe.

Essential Entity Recognition:

Digital infrastructure, crucial for modern society, recognized as essential entities under NIS2. Acknowledges the sector's significance in supporting the modern economy.

Security Upgrades:

NIS2 mandates enhancements to physical security measures, requiring installations like security cameras. Acknowledges the risk posed by physical security threats to organizations in the digital infrastructure sector.

Incident Response Planning:

Organizations must develop robust incident response and recovery plans. Identification of response leaders, rapid information sharing, and evidence-gathering procedures are crucial.

Regulatory Oversight:

Anticipated increase in regulatory oversight as EU authorities enforce NIS2 requirements. Companies held accountable for safeguarding critical systems and networks.

More information

NIS2 Implications:

- Focus on upgrading physical security measures to counter evolving threats.
- Emphasis on incident response and recovery planning for effective cybersecurity measures.
- Anticipated heightened regulatory oversight to ensure compliance.

Cybersecurity Challenges:

- Ransomware threats, shortage of cybersecurity professionals, third-party vendor risks, physical security concerns, IoT vulnerabilities, and compliance complexities.
- Diverse challenges make the sector a high-value target for malicious actors.

Market Impact:

- NIS2 expected to drive demand for innovative cybersecurity solutions.
- Encourages competition and innovation in the digital infrastructure sector, fostering a level playing field.

NIS2: Digital Providers

Importance Recognition:

Digital providers sector, offering diverse digital products, deemed important entities under NIS2. Integral part of the modern digital economy, transforming communication, transactions, and information access.

Sector Overview:

Encompasses search engines, online markets, and social networks. Influential in shaping online interactions for individuals and businesses.

International Impact:

NIS2's impact extends beyond the EU, affecting global digital service providers. Providers need to assess compliance impact on operations outside the EU, considering potential global regulatory shifts.

Greater Accountability:

Transparency and collaboration priorities under NIS2. Reporting significant security incidents and maintaining records enhance accountability, ensuring security obligations are prioritized.

Improved Data Privacy:

Interrelation between NIS2 and data privacy regulations, including GDPR. Compliance with NIS2 improves data privacy and protection standards in the digital providers sector.

More information

NIS2 Implications:

- NIS2 imposes obligations on digital service providers, emphasizing accountability and transparency.
- Collaboration with national cybersecurity authorities, reporting security incidents, and maintaining thorough records are key requirements.

Cybersecurity Challenges:

- DDoS attacks, privacy concerns, phishing attacks, social engineering risks, malware and ransomware threats, and cloud security risks.
- Operational consequences and sensitive data protection are major challenges for web-based services.

Market Impact:

- NIS2 simplifies compliance for digital service providers, harmonizing cybersecurity standards across the EU.
- Encourages providers to prioritize security, enhancing the overall security and resilience of the digital ecosystem.

NIS2: Water Supply

Sector Overview:

Water supply sector categorized as "essential" under NIS2. Critical role in providing communities with clean and safe water, managing wastewater

Included in this sector: Drinking water and wastewater management.

NIS2 Implications:

NIS2 emphasizes protection of critical infrastructure, including water treatment and distribution systems. Water utilities may need substantial cybersecurity investments for resilience against cyber threats.

Coordination with Other Sectors:

Directive stresses coordination between sectors for a comprehensive cybersecurity approach. Water utilities must collaborate with other sectors to develop coherent cybersecurity strategies and ensure compliance.

Risk Management for OT Systems:

Heavy reliance on OT systems in the water sector for critical processes. NIS2 requires water utilities to implement risk management processes specifically for OT systems, ensuring adequate protection against cyber threats.

Critical Infrastructure Status:

Water supply sector categorized as "essential" under NIS2. Critical role in providing communities with clean and safe water, managing wastewater.

More information

Key Cybersecurity Challenges:

- Legacy systems with hidden vulnerabilities.
- Physical security risks in remote or unsecure areas.
- Limited resources for investing in cybersecurity personnel.
- Insider threats by employees or contractors.
- Third-party risks with potential entry points for attackers.
- Control systems susceptible to cyber attacks.

Market Impact:

- Directive impact varies based on unique market conditions and regulatory environments.
- Stimulates demand for cybersecurity services, promotes competition, innovation.
- Water utilities may need to adjust procurement practices to comply with NIS2 cybersecurity requirements.
- Overall impact influenced by specific country market conditions and regulatory environments.

NIS2: Finance

Sector Overview:

Finance sector crucial for managing and supporting the flow of capital. Integral component of the European economy.

Included in this Sector: Banking and financial market infrastructure.

Ensuring Business Continuity:

NIS2 acknowledges the need for continuous availability of financial networks and information systems. Requires financial institutions to have contingency plans for business continuity in the event of a cyber attack. Includes regular testing of plans and measures to minimize the impact of disruptions.

Protecting Financial Data:

Financial institutions must implement robust security measures to protect sensitive financial data. NIS2 mandates encryption of data in transit and at rest, access controls, and regular monitoring for unauthorized access or manipulation of data.

Managing Third-Party Risks:

Finance sector often relies on third-party providers. NIS2 requires assessment and management of risks associated with third-party relationships. Involves regular security assessments, ensuring third-party providers have adequate cybersecurity measures, and implementing contracts requiring NIS2 compliance.

More information

NIS2 Implications:

- Finance sector's handling of sensitive financial information and high-value transactions makes security breaches critical.
- NIS2 requires organizations in the EU finance sector to enhance security and resilience of critical systems and networks.

Cybersecurity Challenges:

- Compliance with the Digital Operational Resilience Act (DORA) following the Commission Guidelines issued on September 18th.
- Phishing attacks targeting online banking systems.
- DDoS attacks disrupting high-value transactions.
- Web-based attacks exploiting vulnerabilities in financial web applications.
- Supply chain attacks compromise financial systems + data.
- Social engineering attacks exploiting human weaknesses.

Market Impact:

- Higher standards improve cybersecurity measures, enhancing security of financial transactions and protecting sensitive financial data.
- Reduces the risk of cyber threats, leading to a more secure finance market and increased confidence in financial institutions.

NIS2: Food

Sector Overview:

EU food sector, covering farming, processing, packaging, transportation, and retail. Essential industry contributing significantly to the European economy.

Included in this sector: Food processing, agriculture, packaging, transportation, and retail.

Focus on Food-Specific Threats:

NIS2 recognizes unique threats in the food sector, such as physical attacks and contaminants. "Important entities" must perform risk assessments considering sector-specific vulnerabilities.

Supply Chain Management:

NIS2 encourages robust supply chain management for cybersecurity. Organizations ensure suppliers and partners meet cybersecurity standards. Leads to a more rigorous vetting process and increased collaboration for cybersecurity best practices.

Better Collaboration on Food Safety:

NIS2 fosters stronger collaboration among EU Member States and international partners. Enhances cybersecurity and encourages the development of global standards, best practices, and initiatives. Promotes increased cooperation on food safety issues for public health and safety.

More information

NIS2 Implications:

- Rising cyber threats due to digitization and interconnectivity.
- NIS2 directive addresses specific risks in the food sector across the EU.

Cybersecurity Challenges:

- Supply chain complexity with millions of small organizations.
- Increasing reliance on vulnerable IoT devices.
- Frequent targeting by ransomware attacks.
- Limited budget for cybersecurity measures.
- Dependence on legacy systems.
- Vulnerabilities through third-party access.

Market Impact:

- NIS2 directive requires investments for compliance, potentially increasing costs.
- Smaller organizations may find compliance challenging due to financial constraints.
- Possible industry consolidation with larger players dominating the market.

NIS2: Health

Sector Overview:

Healthcare sector, including public and private healthcare providers, medical equipment, medicine manufacturers, and medical insurance providers. A cornerstone of European society and economy.

Included in this sector: Public and private healthcare providers, medical equipment and medicine manufacturers, medical insurance providers.

Protection of Patient Data:

NIS2 mandates cyber risk management measures for patient data protection. Clear incident-reporting process implementation. Secure patient data storage and handling practices.

Prevention of Health Service Disruption:

Measures to minimize the risk of disruptions in essential healthcare services. Regular testing and updates of cybersecurity systems. Staff training on cyber hygiene and incident response planning.

Compliance and Enforcement:

Healthcare organizations must comply with strict data privacy regulations like GDPR and HIPAA. NIS2 adds additional cybersecurity regulations, posing challenges for compliance.

More information

NIS2 Implications:

- Healthcare sector categorized as essential, subject to the toughest NIS2 requirements.

Cybersecurity Challenges:

- Lack of standardization in security measures.
- Handling sensitive patient information targeted by cybercriminals.
- Use of outdated technology in healthcare organizations.
- Limited resources and understaffed IT teams.
- Increased risk due to interconnected systems.
- Insufficient cybersecurity training for healthcare employees.

Market Impact:

- Potential increase in healthcare delivery costs for compliance.
- Expected long-term benefits include enhanced security, better protection of patient data, and increased trust in digital healthcare services.

NIS2: Manufacturing

Sector Overview:

Critical part of the European economy, ranging from small-scale production to large-scale industrial processes. Increasing digitization and interconnectivity pose cybersecurity risks.

Included in this sector: Manufacturing of medical devices, computers and electronics, machinery and equipment, motor vehicles, trailers and semi-trailers, and other transport equipment.

Improved Supply Chain Security:

NIS2 directive prioritizes supply chain security. Manufacturers must assess and mitigate risks to the supply chain. Secure suppliers, partners, and contractors with robust cybersecurity measures. Regular assessments to prevent the entire ecosystem from cyber threats.

More Focus on Risk Management:

Manufacturing entities recognized as "important" must implement risk management processes. Investment in new risk management tools and processes. Hiring additional staff with expertise in managing evolving risks.

Increased Collaboration with IT Providers:

Closer collaboration with IT service providers, such as MSSPs and cloud service providers. Potential increased costs and changes to business models and processes.

More information

NIS2 Implications:

- Manufacturing sector categorized as an "important entity" under the NIS2 directive.

Cybersecurity Challenges:

- Phishing attacks targeting valuable data.
- Supply chain attacks on third-party vendor.
- Intellectual property theft for trade secrets and competitive advantage.
- Vulnerabilities in Industrial IoT devices.
- Ransomware attacks impacting production timelines.
- Equipment sabotage causing disruption.

Market Impact:

- Anticipated substantial impact on the manufacturing market.
- Mandates manufacturers to invest in compliance measures.
- Potential budget reallocation towards cybersecurity initiatives.
- Impact on competitiveness and industry consolidation as smaller companies may struggle with additional costs.

NIS2: Postal

Sector Overview:

Diverse organizations responsible for mail and parcel delivery, from national postal services to niche courier companies. Increased reliance on digital systems and networks, making the sector susceptible to cyber threats.

Included in this sector: Postal and courier services.

Increased Customer Data Protection:

Postal operators handle significant personal data. NIS2 requires robust cybersecurity measures, including encryption and access controls. Data breaches could have severe consequences for both customers and operators.

More Stringent Supplier Security:

Heavy reliance on a wide range of suppliers and partners. NIS2 mandates assessment and mitigation of cybersecurity risks in the supply chain. Increased oversight and auditing of suppliers, implementing stringent security requirements.

Greater Industry Collaboration:

NIS2 emphasizes cooperation and information-sharing within the sector. Potential collaboration between postal operators for sharing threat information and best practices. Development of sector-specific guidelines and standards for cybersecurity.

More information

NIS2 Implications:

- Postal sector recognized as an "important entity" under the NIS2 directive.

Cybersecurity Challenges:

- Ransomware attacks causing disruptions to postal services.
- Damaging malware infections leading to data loss or extended downtime.
- Vulnerabilities in a complex supply chain network.
- Lack of cybersecurity awareness among employees and management.
- Common phishing attacks targeting employees.
- Insider threats from employees or contractors with system access.

Market Impact:

- Compliance with NIS2 may result in increased costs and administrative burdens.
- Potential impact on cross-border package delivery and a more fragmented market.
- Focus on supply chain security may require rigorous assessments of suppliers and partners, leading to increased oversight and auditing of supply chain security.

NIS2: Public Administration

Sector Overview:

Critical component of European society, providing essential services such as social services, public safety, economic regulation, and political representation. High risk of devastating attacks due to vast amounts of sensitive information.

22.1% of GDP - Average annual government expenditure on public services of EU countries.

Protecting Sensitive Information:

NIS2 requires enhanced security measures to protect sensitive citizen information, financial data, and critical infrastructure. Particularly crucial for the public administration sector due to the handling of vast amounts of sensitive information.

Continual Risk Assessment:

Public administration organizations mandated to conduct regular risk assessments and report on cybersecurity posture. Ensures identification of areas for improvement in cybersecurity measures. Aims to ensure availability and functionality of essential public services even in the event of a cyber incident.

Raising Employee Awareness Level:

NIS2 compliance requires investment in employee cybersecurity training. Critical given varying degrees of cyber awareness among employees, representing a significant security risk.

More information

NIS2 Implications:

- Public administration sector designated as an "essential entity" under the NIS2 directive.

Cybersecurity Challenges:

- Limited IT resources and challenges in recruiting cybersecurity talent.
- Prime target for phishing attacks due to vast amounts of personal data.
- Deployment of large, complex IT systems vulnerable to cyberattacks.
- Lack of cybersecurity awareness among employees.

Market Impact:

- Mandates best practices for safeguarding against cyber threats, ensuring availability of essential services.
- Focus on employee education and regulatory compliance strengthens sector's defenses.
- Regular risk assessments and incident response planning enhance vigilance and preparedness against evolving cyber threats.

NIS2: Research

Sector Overview:

Valuable contributor to innovation and progress. Target for cybercriminals seeking to steal sensitive research data or disrupt critical systems. Recognized as critical infrastructure under the new NIS2 Directive.

€311 billion - Annual expenditure on Research & Development (R&D) in Europe.

Research Jobs In EU:

2 million+ - Number of full-time researchers in the EU research sector.

International Compliance Challenges:

NIS2 requirements differing from other countries' regulations pose compliance challenges for international collaborations. Impact on pace and scope of collaborations, particularly for smaller organizations struggling with multiple regulatory regimes.

Improved Data Protection and Privacy:

Significant implications for handling sensitive data, including personal health information and intellectual property. Compliance with multiple regulations, such as GDPR and NIS2, required to ensure data protection. Potential challenges in sharing data across borders, impacting research collaboration.

More information

NIS2 Implications:

- Research sector categorized as a critical infrastructure sector under NIS2.

Cybersecurity Challenges:

- Intellectual Property Theft: Valuable intellectual property targeted for theft.
- Ransomware Attacks: Potential for devastating impact, forcing organizations to pay large ransoms.
- Data Breaches: Highly confidential research data loss leading to reputational damage and funding loss.
- Legacy Systems: Reliance on outdated systems susceptible to attacks due to lack of regular updates.
- Insider Threats: Authorized personnel may misuse access, leading to data leaks.
- Third-party Risk: Partners providing critical services may lack cybersecurity standards.

Market Impact:

- Likely investment in additional security measures and staff to ensure compliance with NIS2.
- Non-compliance may result in fines and penalties, creating financial risks.
- Emphasis on collaboration and information sharing leads to stronger cybersecurity within research organizations, benefiting the research community.

NIS2: Space

Sector Overview:

Essential component of the modern economy, critical to telecommunications, navigation, and national security. Prime target for cyber threats due to its significance.

Reporting Requirements:

NIS2 introduces new reporting requirements for space organizations. Reporting cyber incidents impacting space infrastructure, including satellites and ground stations. Challenges in monitoring, detecting, and responding to potential cyber threats.

Collaboration with Regulatory Bodies:

Necessitates greater collaboration between the space industry and regulatory bodies. Information and intelligence sharing to improve overall cybersecurity and resilience. Strengthening the sector's ability to identify and address potential cybersecurity risks.

Focus on Supply Chain Security:

Requires space organizations to prioritize supply chain security. Implementation of robust supply chain risk management practices. Due diligence and monitoring of suppliers and third-party contractors.

More information

NIS2 Implications:

- Recognizes the space sector as an essential entity, subject to strict cybersecurity requirements.

Cybersecurity Challenges:

- Sophisticated Cyberattacks: Prime target for nation-state actors and APT groups.
- Legacy Systems: Vulnerability due to decades-old systems not designed for modern cybersecurity threats.
- Supply Chain Risks: Complex global supply chains creating vulnerabilities.
- Limited Visibility: Challenges in detecting and responding to incidents in complex and remote space systems.
- Human Error: Complex systems and high human interaction levels leading to security risks.
- Space-based Asset Threats: Vulnerability of space-based assets to disruptions.

Market Impact:

- Compliance may create new entry barriers in the space market.
- Smaller and newer organizations may find it challenging to comply, potentially leading to market consolidation.
- Changes in the competitive landscape and emergence of new industry leaders prioritizing cybersecurity and resilience.

NIS2: Transport

Sector Overview:

Employing nearly 10 million people, Europe's transport sector is vital for societal and economic connectivity. Encompasses urban public transportation, rural roads, inter-regional air travel, and more.

Operational Technology Security:

Mandates evaluation and control of potential cybersecurity threats from external suppliers. Verification of systems and products meeting security standards. Determining the ability to withstand and recover from a cyberattack.

Protecting Real-Time Data Exchange:

Heavy reliance on real-time data exchange, especially in air traffic control systems. NIS2 requires securing data exchange channels to prevent unauthorized access or manipulation. Implementation of encryption, access controls, and monitoring systems for data integrity.

Safeguarding Supply Chains:

Transportation sector relies on operational technology, such as control systems for trains, ships, and planes. NIS2 directive mandates implementing measures to secure these systems from cyber threats. Implementation of firewalls, access controls, and intrusion detection systems for protection.

More information

NIS2 Implications:

- Transport sector considered essential under the NIS2 directive due to potential destructive ripple effects.

Cybersecurity Challenges:

- Ransomware Attacks: Growing threat disrupting operations and demanding payment.
- Supply Chain Vulnerability: Introduction of vulnerabilities through third-party suppliers.
- Threats To Safety Systems: Safety-critical systems can cause harm if compromised.
- Connected Devices: Increased risk with the use of connected devices like GPS trackers and in-vehicle systems.
- Limited Security Investment: Limited budget and skills gaps due to a focus on optimizing efficiency.

Market Impact:

- Implementation of NIS2 will require transport operators to invest in more effective cybersecurity requirements.
- Potential short-term increase in costs.
- Increased investment expected to result in a more secure and resilient industry in the long run.
- Companies able to invest heavily in security likely to gain a competitive advantage over others.

NIS2: Waste

Sector Overview:

Essential for public health, environmental protection, and sustainability. Involves collecting, transporting, treating, and disposing of waste. Vulnerable to cyberattacks that could disrupt critical operations.

Broader Integration of Cybersecurity:

NIS2 requires integration of cybersecurity into the entire waste management lifecycle. Cybersecurity measures considered at every stage, from waste collection to disposal.

Cyber Awareness Training:

Resource allocation for developing and implementing sector-specific cybersecurity awareness training programs.
Coverage of unique cybersecurity risks associated with waste management operations.

Risk Assessment and Management:

Regular cybersecurity risk assessments and measures to mitigate identified risks. Allocation of resources for assessing and addressing unique cybersecurity risks in waste management.

NIS2 Implications:

- Waste management industry is a new sector covered by the NIS2 Directive.

Cybersecurity Challenges:

- Legacy Systems: Reliance on outdated systems vulnerable to cyber attacks.
- Supply Chain Security: Complex supply chain with multiple partners poses significant challenges.
- Third-party Risks: Vendors may lack cybersecurity standards, creating risks.
- Employee Awareness: Critical for recognizing and responding to potential cyber threats.
- Data Protection: Generation of personal and sensitive environmental data requiring protection.
- Phishing Attacks: Cybercriminals target employees with fraudulent emails or messages.

Market Impact:

- NIS2 implementation requires a proactive approach to cybersecurity, potentially leading to significant changes in business models and practices.
- Impact on innovation as organizations invest in new technologies and processes for compliance.
- Opportunity for organizations to enhance cybersecurity and resilience, improving public health and environmental safety.