Marsh

Getting ready for the NIS 2 Directive (EU)

Marsh Cyber Practice

Contents

A revamped version of the Network and Information Security (NIS) Directive: Expanding scope and strengthening guidelines across EU member states.

As cyberattacks continue to grow in severity and prevalence, the need for stronger rules and guidance on network, information and information system security arises.

Consequently, the European Union implemented a revised version of the 2016 NIS Directive to increase cyber resilience across its member states.

By October 17, 2024, member states are required to have adopted and published measures to comply with NIS 2. A list of essential and important entities must be established by member states under NIS 2 definitions by April 17, 2025.

What's new in NIS 2?

1. **Extended scope**
2. **Strengthened cybersecurity risk management measures**
3. **Improved incident reporting**
4. **Increased penalties**

Scope of application

Essential entities

- Energy
- Transport
- Banking
- Financial markets
- Health
- Drinking water
- Digital infrastructure
- Information and communication technology service management
- Public administration
- Space
- Waste water

Important entities

- Postal and courier services
- Waste management
- Manufacturing
- Digital providers
- Food
- Production, processing, and distribution of food
- Manufacture, production, and distribution of chemicals

NIS 2 expands the scope of the rules to include new sectors and entities. Any large (headcount over 250 or more than €50 million revenue) or medium (headcount over 50 or more than €10 million revenue) enterprise from these sectors will be included in the NIS 2 scope, however member states can extend these requirements and include other critical subjects of choice. Entities in scope will have to comply with the same requirements, but there will be a distinction in supervisory measures and penalties.

Essential entities will be subject to proactive supervision by authorities as opposed to reactive supervision reserved for important entities.

Liability for executives

Executives and top-level leadership within the organisation have a duty to understand the cybersecurity risk their organisation faces, approve strategies and policies to mitigate those risks, and ensure these measures are put into practice. To fulfil their responsibilities, they should also undergo cybersecurity training on a regular basis. In case of cybersecurity breaches, these governing bodies or executives can be held liable.

Strengthened cybersecurity risk management measures

Entities within the scope of NIS 2 must take appropriate and proportionate technical, operational, and organisational measures to manage the risks posed to the security of network and information systems that those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Measures shall include at least:

- Risk assessments and security policies for information systems.
- Policies and procedures for evaluating the effectiveness of security measures.
- Policies and procedures for the use of cryptography and, when relevant, encryption.
- A plan for handling security incidents.
- Security around the procurement of systems and the development and operation of systems, including policies for handling and reporting vulnerabilities.
- Cybersecurity training for basic computer hygiene.
- Security procedures for employees with access to sensitive or important data, including policies for data access. Affected organisations must also have an overview of all relevant assets and ensure that they are properly utilised and handled.
- A plan for managing business operations during and after a security incident, including ensuring access to IT systems and their operating functions during and after a security incident. Backups of systems and data must be kept up to date.
- The use of multi-factor authentication, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, where appropriate.
- Companies must assess the overall security levels of all suppliers and implement appropriate security measures to combat vulnerabilities within their supply chain.

Incident reporting obligations

Essential and important entities must promptly notify their computer security incident response team (CSIRT) or competent authority of significant incidents that impact their services. They should also inform service recipients when necessary:

- Within **24 hours** of identifying a significant incident, provide an early warning, including potential causes and cross-border implications, if applicable.
- Within **72 hours** of identifying a significant incident, submit an incident notification with updates, including severity, impact assessment, and indicators of compromise.
- Provide a final report within one month after the incident notification submission.

Penalties

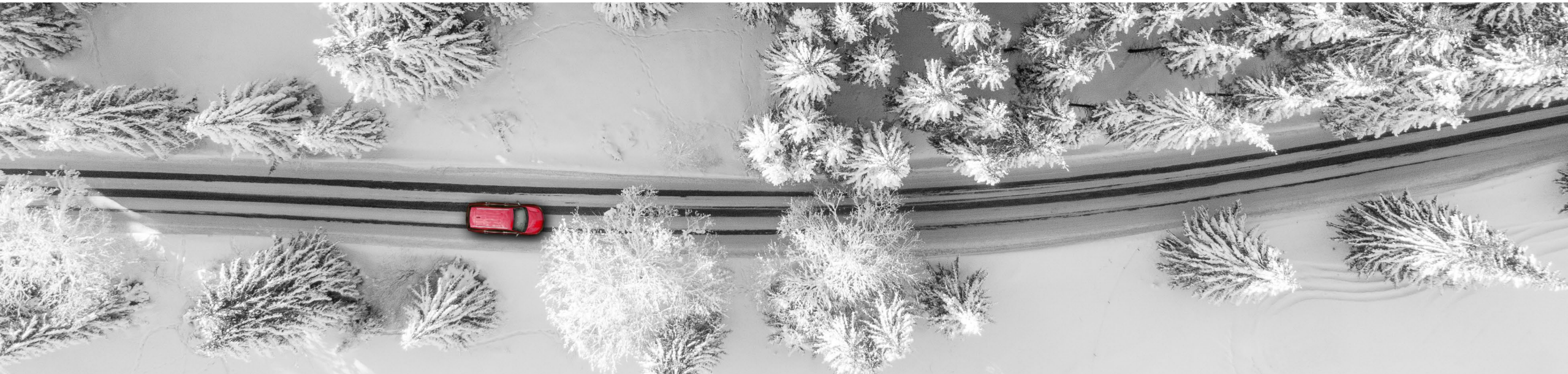
NIS 2 provides a penalty regime according to which, in case of violation of Articles 21 and/or 23:

Essential entities

Essential entities are subject to administrative fines of up to **€10,000,000** or a maximum of at least **2%** of the total annual worldwide turnover for the previous fiscal year of the enterprise to which the essential entity belongs, whichever is higher.

Important entities

Important entities are subject to administrative fines up to **€7,000,000** or **1.4%** of the total annual worldwide turnover in the preceding fiscal year of the enterprise to which the important entity belongs, whichever amount is higher.



How cyber insurance can help with the NIS 2 implications

- **Financial protection**: Cyber insurance provides financial protection by covering the costs associated with cyber incidents, such as data breaches, ransomware attacks, and business interruption. This can include expenses related to forensic investigations, legal fees, notification and credit monitoring services, and public relations efforts.
- **Incident response**: Cyber insurance often includes access to a network of experts who can assist in responding to cyber incidents. This can include forensic investigators, legal counsel, public relations professionals, and IT specialists. These experts can help with incident containment, data recovery, and managing the overall response to the incident, which is crucial for complying with NIS 2 requirements.
- **Risk assessment and mitigation**: Many cyber insurance policies offer risk assessment services to help businesses identify vulnerabilities and implement appropriate security measures. By conducting risk assessments and implementing recommended security controls, businesses can enhance their cybersecurity posture and reduce the likelihood of cyber incidents, thereby aligning with NIS 2 requirements.
- **Business continuity**: Cyber insurance can provide coverage for business interruption losses resulting from cyber incidents. This can include reimbursement for lost income, extra expenses incurred to maintain operations, and costs associated with restoring systems and data. Having this coverage can help businesses meet the NIS 2 requirement of ensuring the continuity of essential services.
- **Regulatory compliance**: NIS 2 imposes certain obligations on businesses, including incident reporting requirements and security measures. Cyber insurance can help businesses meet these obligations by providing guidance on compliance and non-compliance, depending on specific legal requirements.

Cyber insurance is not a substitute for implementing robust cybersecurity measures. It is a complementary tool to help manage and transfer some of the financial risks associated with cyber incidents.

To fully benefit from cyber insurance, businesses should also invest in cybersecurity measures, such as implementing strong access controls, regular security assessments, employee training, and incident response plans.

It’s recommended that (new) cyber insurance buyers consult with insurance professionals who specialise in cyber insurance to understand the specific coverage options available and how they align with NIS 2.

How Marsh can help

Our wide range of cyber risk solutions offer valuable support and expertise to facilitate your journey towards NIS 2 compliance.
We will help you identify your current cyber risk posture and give you a clear view on cyber investment decisions. We can help you by:

Providing expert advice and guidance on your cyber risks through a risk assessment and quantification.

Assisting you in anticipating NIS 2 risk management measures such as incident management and business continuity.

Enhancing your overall cyber resilience through services such as penetration testing, phishing training, and vulnerability management.

Accessing proprietary insurance programmes, products, and tools to inform and improve cyber risk transfer.

Contact the experts

For more detailed information, contact our experts:

Gregory van den Top
Head of Cyber Risk Consulting, Europe

+31 (0)6 12 56 89 72
gregory.vandentop@marsh.com

Sjaak Schouteren
Cyber Growth Leader
Marsh Europe

+31 (0)6 53 81 72 82
sjaak.schouteren@marsh.com

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With more than 45,000 colleagues advising clients in over 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue of $23 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. For more information, visit marsh.com, and follow us on LinkedIn and X.