Get an overview of the potential penalties from NIS2 non-compliance

What is NIS2?

The NIS2 Directive builds upon the foundation laid by its predecessor, maintaining its core objective: safeguarding critical infrastructure and organizations within the EU from cyber threats and ensuring a high, uniform level of cybersecurity across member states.
To achieve this goal, NIS2 requires member states to take a number of additional measures, including:

- Establishing an incident response plan that coordinates with other member state plans.
- Establishing a national Computer Emergency Response Team.
- Strengthening cooperation between public and private sector entities.
- Improving information sharing between member states.

Through these measures, and by offering support and guidance to both businesses and individuals, the EU aims to bolster collective resilience against cyberattacks and better protect its citizens from the increasing dangers of the digital world.

Consequences of NIS2 Non-Adherence

The NIS2 Directive outlines clear consequences for breaches, encompassing:

- Remedies that don't involve money
- Financial penalties
- Legal repercussions

Both essential and important entities may face these consequences for lapses such as not adhering to security protocols or neglecting to report certain incidents.

Non-Financial Penalties

NIS2 empowers national oversight bodies with the ability to levy non-financial penalties, which include:

- Orders to comply
- Direct mandatory instructions
- Mandates for security audits
- Alerts to an entity's clients about potential risks.

Financial Penalties Overview

The NIS2 directive clearly differentiates the financial penalties for essential versus important entities:

- Essential Entities: Member States are directed to levy fines up to the greater of €10,000,000 or 2% of the global yearly revenue.
- Important Entities: Under NIS2, the fines can reach up to either €7,000,000 or 1.4% of the annual global revenue, with the higher amount being applicable.

Criminal Sanctions For Management

In an attempt to lower the pressure put on IT departments to single-handedly ensure the security of the organization and to change the sentiment of whose responsibility cybersecurity is, NIS2 includes new measures to hold top management personally liable and responsible for gross negligence in the event of a security incident.

Specifically, NIS2 allows Member State authorities to hold organization managers personally liable if gross negligence is proven after a cyber incident. This includes:

- Ordering that organizations make compliance violations public.
- Making public statements identifying the natural and legal person(s) responsible for the violation and its nature.
- And if the organisation is an essential entity, temporarily ban an individual from holding management positions in case of repeated violations.

By targeting corporate leadership, these provisions seek to strengthen accountability and prevent severe mismanagement of cybersecurity threats.

Important Entities (IE)

This group covers both public and private enterprises in industries including food production, digital services, chemicals, postal operations, waste management, research, and manufacturing sectors.

Penalty Threshold: Either €7 million or 1.4% of the total annual global revenue, whichever is greater.

Essential entities (EE)

This category encompasses both public and private sector organizations operating in fields like transportation, finance, energy, water, aerospace, healthcare, public governance, and digital Infrastructure

Potential Fine: The higher of €10 million or 2% of their yearly global turnover.