Your Damen guide to navigating cyber security regulations

DAMEN

Introduction

In today's increasingly connected world, the shipping industry faces a growing array of cyber security threats that can have significant implications for global trade. Recent disturbances like the 2021 Suez Canal blockage and the rise in ransomware attacks highlight the sector's vulnerability. The local cyber-attack on the city of Antwerp in 2022 caused damages up to € 100 million. The global cyber-attack *NotPetya* in 2017 that also hit Maersk, reportedly cost the company € 300 million. Even more threatening, in 2021 Russia spoofed the presence of NATO ships visiting Ukraine in the Black Sea increasing military tensions.

Cyberattacks like ransomware can halt navigation systems or compromise critical onboard controls. Classified as critical infrastructure, shipping has seen a drastic surge in security breaches costing shipowners on average up to € 550 thousand per breach. These developments underscore the urgent need for robust cyber risk management to safeguard the maritime industry's critical infrastructure and ensure uninterrupted operations.

How do these incidents get so costly? A survey among 489 maritime professionals from 50 countries for their Maritime Cyber Priority report and found that 31% have experienced at least one infiltration by attackers in the last twelve months, with the average incident taking 57 days to resolve. A study found in 2021 that 95% of cyber incidents can be linked to an unintentional insider (i.e. a software misconfiguration), showing the lack of cyber risk management. What is perceived as an ever stronger driver to trigger cyber security investments than a recent cyber incident, is regulation and compliance.

To address these issues, the International Association of Classification Societies (IACS) has introduced two critical unified requirements (URs) to bolster the cyber resilience of ships: IACS E26 and IACS E27. Additionally, the EU has developed the NIS2 Directive to further enhance cyber security across the region. Here's an overview of these regulations and their impact on shipowners.

IACS E26: Cyber resilience of ships

IACS E26 focuses on the ship as a whole, aiming to ensure the secure integration of both operational and information technology (OT & IT) equipment into the vessel's network during its design, construction, commissioning, and operational life.

It covers five key aspects of cyber security:
Identify: Ensuring all equipment is accounted for and recognised within the system.
Protect: Implementing measures to safeguard the ship's systems.
Detect: Establishing mechanisms to identify potential cyber threats.
Respond: Developing protocols to address and mitigate the effects of cyber incidents.
Recover: Creating strategies to restore systems to normal operation after an incident.

IACS E27: Cyber resilience of on-board systems and equipment

IACS E27 targets the system integrity of all individual vessel equipment and its suppliers. It provides requirements for the cyber resilience of onboard systems and equipment, emphasising the interface between users and computer-based systems onboard, as well as product design and development requirements for new devices before their implementation onboard ships.

	IACS E26	IACS E27
Covers	Cyber Resilience of Ships	Cyber Resilience of On-Board Systems and Equipment
Applies to	For all newbuilds contracted since mid-2024 • Passenger ships (including passenger high-speed craft) engaged in international voyages • Cargo ships of 500 GT and upwards engaged in international voyages • High speed craft of 500 GT and upwards engaged in international voyage • Mobile offshore drilling units of 500 GT and upwards • Self-propelled mobile offshore units engaged in construction (i.e. wind turbine installation • maintenance and repair, crane units, drilling tenders, accommodation, etc.)	
Requirements	• Design assessment for secure communication, authentication and access control • Regular assessment of ship system vulnerabilities • Documentation of software configurations and updates • Documentation and control over network remote access	
Non-compliance	• Denial of classification or certification • Vulnerability to cyber attacks • Fines from maritime regulators (flag states, port authority) • Costs for getting ships to comply retroactively	

NIS2 Directive: A high common level of cyber security in the EU and UK

The NIS2 Directive entered into force in the EU on January 16, 2023, with member states required to adopt and enforce the directive by October 2024. It requires member states to strengthen cyber security capabilities and introduces cyber security risk-management measures and reporting in critical sectors, along with rules on cooperation, information sharing, supervision, and enforcement. The directive applies to a wide range of sectors, including maritime transport, and obliges more entities to take measures to increase the level of cyber security in Europe.

Impact on shipowners
For shipowners, these regulations represent a significant step towards ensuring the safety and security of their vessels in the face of evolving cyber threats. The impact of IACS E26, E27, and NIS2 can be summarised as follows:

- **Enhanced security:** Shipowners can be confident that their vessels are built with a robust cybersecurity framework, reducing the risk of cyber incidents.
- **Standardised requirements:** The URs provide a clear and standardised set of requirements, simplifying the process of ensuring compliance and enhancing cyber resilience.
- **Industry feedback integration:** The regulations have been refined based on industry feedback, ensuring they are practical and effective in real-world applications.
- **Future-proofing:** By adhering to these requirements, shipowners will be better prepared for future technological advancements and the associated cyber risks.

	EU NIS and NIS2	UK NIS
Applies to	Critical infrastructure: transport, energy, health, finance	
In effect since	• NIS in 2016 • NIS2 in 2023, member state enforcement October 2024	• Adopted in 2018
Requirements	• Incident response (<24 hours) • Supply chain risk management	• Similar to EU NIS but softer than EU NIS2
Non-compliance	• Up to €10m or 2% revenue • Management accountable and personally liable for damage	-
Proposed updates	-	• Penalties up to £ 17m • Management liability & incident response similar to EU NIS2

Consequences of non-compliance

Non-compliance with IACS E26, E27, and NIS2 can have serious repercussions for shipowners:

Increased vulnerability: Ships that do not meet the cyber resilience standards are more susceptible to cyber-attacks, which could compromise safety and operational integrity.

Regulatory penalties: Shipowners may face penalties from regulatory bodies for failing to comply with the mandatory requirements, with fines of up to 10 million euros or 2% of global revenues.

Insurance implications: Non-compliance could affect insurance coverage, as insurers may view non-compliant ships as higher risk.

Operational disruptions: Cyber incidents resulting from non-compliance can lead to significant operational disruptions, financial losses, and reputational damage.

Survey and certification issues: Ships that do not comply with the URs may encounter difficulties during surveys and certification processes, potentially leading to delays in vessel delivery or operation.

Legal liabilities: Shipowners could be held liable for damages resulting from cyber incidents, especially if it is found that non-compliance contributed to the incident. Additionally, senior management could face personal liability claims if it is determined that negligence in implementing adequate cyber resilience measures contributed to a cyber incident. This could include fines and, in extreme cases, criminal charges if wilful misconduct is proven.

Damen Triton Cyber security

Without robust cyber resilience, vessels are at risk for unplanned downtime, ransom attacks, and regulatory non-compliance. Already close to 800 vessels have been securely connected to the Damen Triton platform, mitigating cyber security risks. The Damen Triton platform provides cyber security solutions for its customers and provides consultancy services on how to make customer fleets cyber resilient.

Damen Triton's cyber security solution includes:

- **Network Cyber Resilience:** Secured on-board data collection, storage, access, cloud connection and distribution to shore – Damen Triton is Bureau Veritas type approved for cyber resilience.
- **Cyber Regulation Support:** Supporting shipping companies to identify all internet connected ship systems and applications for their cyber security fleet plan.
- **Damen Triton Guard:** Controlled Remote access giving remote access to any connected onboard systems, in line with IACS and EU NIS2 cyber security regulations.

Looking to secure your fleet? Get in touch with the Damen team for more information at sales.triton@damen.com

DAMEN

Damen.com