



## Cyber security controls for existing ships

While mandatory cyber resilience requirements primarily apply to newbuilds, cyber threats affect ships regardless of age. IACS Recommendation No. 194 provides a practical baseline for strengthening cyber security controls across existing fleets.

Published 05 October 2026

The information provided in this article is intended for general information only. While every effort has been made to ensure the accuracy of the information at the time of publication, no warranty or representation is made regarding its completeness or timeliness. The content in this article does not constitute professional advice, and any reliance on such information is strictly at your own risk. Gard AS, including its affiliated companies, agents and employees, shall not be held liable for any loss, expense, or damage of any kind whatsoever arising from reliance on the information provided, irrespective of whether it is sourced from Gard AS, its shareholders, correspondents, or other contributors.

[Cyber Security Awareness Month](#) in October offers an opportunity to reflect on the evolving cyber threat landscape facing the maritime sector. Although much attention is currently focused on the opportunities and risks associated with artificial intelligence (AI) and other emerging technologies, many cyber incidents still stem from basic security weaknesses and shortcomings in cyber hygiene.

Addressing these basic weaknesses is particularly relevant as digital systems and software support critical shipboard functions, including navigation, communication, monitoring, ballast water management, cargo handling, propulsion and steering. Their increasing connection to shore-based networks, remote support services and other external interfaces makes cyber security an important part of safe and reliable ship operation.

## Maritime cyber threat trends

The [U.S. Coast Guard's](#) *Cyber Trends and Insights in the Marine Environment 2025* report and [France Cyber Maritime's](#) *Maritime Cyber Threat Overview 2025* both show that maritime cyber incidents remain on an upward trend, creating an increasingly challenging operating environment for shipowners, operators and port facilities. At the same time, they continue to highlight many of the underlying vulnerabilities that have affected the sector for years. Persistent challenges include phishing, poor credential practices, exposed remote services, outdated software and insufficient network segregation, particularly in operational technology (OT) environments.

Against this backdrop, both reports address growing interest in AI and its potential impact on maritime cyber risk. Although concern is increasing about its possible misuse by cybercriminals, the French report notes that none of the maritime incidents reviewed in 2025 involved AI-driven attacks. For now, AI appears to be helping attackers scale established techniques such as phishing, fraud and malicious scripting rather than fundamentally changing the threat landscape. The French report also highlights its growing role in cyber defence, particularly in security testing and helping teams identify and prioritise potential threats. The U.S. report similarly notes that properly implemented and configured AI-enabled security tools can be highly effective. Together, the reports suggest that technological advances can strengthen cyber resilience but do not replace sound cyber security practices and effective risk management.

## IACS guidance helps close the gap for existing ships

The International Association of Classification Societies (IACS) released its [Unified Requirements E26 and E27](#) on the cyber resilience of ships in 2023. However, since these apply only to new ships contracted for construction on or after 1 July 2024, IACS has also published [Recommendation No. 194, Cybersecurity Controls for Existing Ships \(Rec. 194\)](#). Rec. 194 helps address this gap by providing a minimum baseline of cyber security controls for ships contracted before this date, supporting a more consistent level of cyber resilience across existing fleets. It complements other IACS unified requirements and recommendations on cyber resilience.

IACS describes cyber resilience as the capability to reduce the occurrence and mitigate the effects of cyber incidents arising from disruption or impairment of OT used for the safe operation of a ship, where such incidents could lead to risks to people, the ship or the environment.

Cyber resilience is therefore not only a technical matter or a question of preventing unauthorised access to individual systems. It is about maintaining safe operation when critical OT systems or supporting connections are disrupted, compromised or unavailable. This requires planning for incidents that affect several systems or supporting functions at the same time and ensuring that critical systems can be restored or operated safely in degraded mode. Rec. 194 supports this by setting out controls covering management responsibility, cyber risk assessment, network protection, system maintenance, monitoring, response and recovery, as well as familiarisation and training for crew.

For existing ships, this means looking beyond individual systems and considering how cyber risk is managed across ship operations, procedures and shore support arrangements. A key area to review is the connection between onboard IT and OT systems. While Rec. 194 addresses both, its primary focus is on OT systems and their possible connections to IT systems, as these may directly support safe ship operation. IACS recognises that many existing ships may have been built before cyber risks linked to IT/OT interconnections were fully considered. Where this is the case, IACS recommends separating OT systems from IT systems.

IACS also recommends that companies incorporate periodic assessments into their overall cyber security strategy to address emerging risks and verify alignment with industry best practices and regulatory requirements.

## **Cyber resilience in practice: what operators should consider**

In practical terms, Rec. 194 can help ship operators assess whether appropriate cyber security measures are in place and identify where additional safeguards may be needed. As a starting point, they may wish to ask: **Identify** : Have we identified the onboard IT and OT systems, software, interfaces, and data flows that support safe ship operation? **Protect** : Are appropriate safeguards in place, including strong authentication, secure remote access, network segregation between IT and OT environments, malware protection, vulnerability and patch management, protection of sensitive data, and crew awareness and training? **Detect** : Do we have arrangements to monitor systems and identify unusual activity, unauthorised access attempts, system malfunctions, or other signs of possible compromise? **Respond** : Are cyber incident response, reporting and escalation and decision-making processes clearly defined, understood, and tested onboard and ashore? Do personnel know how to recognise and report potential cyber incidents? **Recover** : Do we have tested backup, restoration and recovery arrangements for systems and data needed for safe ship operation, and are they protected from the same incident affecting the primary systems?

## Regulatory direction

Maritime cyber regulation is developing on several fronts. IMO's revised [Guidelines on Maritime Cyber Risk Management](#) , issued as MSC-FAL.1/Circ.3/Rev.4 in May 2026, continue to provide a high-level international framework for managing cyber risk as part of safe and secure shipping operations. The guidelines emphasise integration with company processes such as safety management, security management, risk assessment, training, incident reporting and contingency planning. IMO has also agreed to develop a goal-based, non-mandatory Maritime Cyber Code, with a target completion date in 2028.

Alongside non-mandatory guidance, cyber security requirements are becoming more specific and verifiable. IACS' cyber resilience requirements for newbuilds are one example. Another is the mandatory cyber security regime established under 33 CFR Subpart F for certain U.S.-flagged vessels and facilities. Under these regulations, vessel operators within scope must develop and maintain an approved cyber security plan, designate a cyber security officer, and conduct regular assessments, exercises and audits. This development signals a shift towards a more prescriptive and structured framework, with greater emphasis on specific controls, governance arrangements and regulatory oversight.

## Building cyber resilience

In summary, cyber resilience is the ability to anticipate, withstand, adapt to, and recover from cyber incidents and disruptions. Gard encourages ship operators to make cyber risk management part of everyday operations, covering processes, technology and people. In light of growing geopolitical tensions, increasing digital interconnectivity, and the potential misuse of AI by cyber attackers, a structured approach to cyber risk management is becoming an essential part of safe and secure shipping.

Although IACS Rec. 194 is not mandatory, it provides a useful benchmark for reviewing whether cyber security arrangements are suitable for the systems, operations and shore-based connections in place across a fleet. Used alongside the revised IMO guidelines, class and flag requirements, and other relevant industry standards, it can help operators identify and address gaps that may expose ships to operational disruption, safety risks or business continuity challenges.

*For further information, see Gard's "[Cyber security](#)" webpage.*