LP 34/2026 Cyber Intrusions Come Aboard: From Ransomware to Takeover of Safety-Critical Systems

A decade of digital transformation has networked the modern ship. ECDIS, integrated bridge systems, main engine remote controls and cargo management systems all ride the same data highways, linked to shore offices and the wider internet via satellite. Efficiency has soared but so has exposure: ships are now permanently online, remotely accessible nodes. Geopolitical spill-over has raised the stakes further, with state-sponsored APTs, GPS jamming and spoofing, and malware implants joining the threat landscape. Attackers are no longer just after money — they seek strategic leverage, infrastructure disruption and geopolitical advantage. Cyber risk has moved ashore to on board, and maritime cyber defence is now a strategic priority.

I. A Rising Threat

Shore-based cyber-attacks typically stop at data encryption and business interruption. The real gamechanger is that attackers are now targeting the ship itself. A string of incidents from authorised penetration tests to real intrusions shows that OT-level breaches are no longer theoretical. Key incidents in recent years:

- **Jun 2017 — Maersk / NotPetya:** The NotPetya ransomware attack knocked out IT systems across multiple sites and business units, costing an estimated USD$300 million. The shipping industry saw first-hand the scale of damage a cyber-attack could inflict.
- **Dec 2017 — Naval Dome live test:** Israeli cybersecurity firm Naval Dome demonstrated on a live vessel that a single phishing email to the master could shift the reported GPS position, inject false radar targets, disable machinery monitoring, and override fuel and ballast pump controls. The test proved that cyber-attacks could threaten physical safety, not just data confidentiality.
- **Feb 2019 — Deep-draft vessel, New York:** A deep-draft ship bound for New York and New Jersey suffered a significant cyber incident affecting its onboard network. The US Coast Guard issued Marine Safety Alert 06-19: malware had severely degraded the computer system, though essential controls were unharmed. The vessel was operating without effective cyber safeguards, leaving critical systems exposed.

- **Jan 2023 — DNV ShipManager ransomware:** Ransomware hit DNV's ShipManager servers, affecting around 70 customers and nearly 1,000 vessels. The entire server environment had to be rebuilt from scratch.
- **Dec 2025 — GNV *Fantastic*:** A Remote Access Trojan (RAT) was discovered in the electronic systems of the Italian ferry GNV *Fantastic* (2,000+ passengers) while docked in Sète, France. A Latvian crew member was charged with computer intrusion for the benefit of a foreign power; France's interior minister cited suspected foreign interference. The ship resumed sailing after a full security inspection.
- **Aug 2026 — *VL Prosperity*:** The VLCC *VL Prosperity* (2.3 million barrels of oil) suffered a suspected cyber intrusion in the Strait of Gibraltar, with communications disrupted for about 30 hours. US Coast Guard Cyber Protection Team and FBI Cyber Action Team personnel boarded on 21 August to inspect OT and IT systems. An LNG carrier was also inspected three days after a suspected attack; its manager confirmed normal operations had resumed.
- **Sep 2026 — *Vivit Africa*:** The 174,000-cbm LNG carrier *Vivit Africa*, carrying US LNG to Italy, reported losing access to part of its internal control systems. Attackers gained temporary control of steam-pressure and safety-valve systems in the Strait of Gibraltar, then compromised tank-pressure controls, pressure-relief valves and the BOG management cycle as the vessel neared the Adriatic. The ship abandoned its planned discharge near Rovigo and diverted west toward Spain with its cargo still on board.

II. Safety & Liability Implications

A cyber-attack on a ship is not just an IT problem. The risks and consequences now unfolding map directly onto traditional maritime risks.

1. Vessel and crew safety

If an LNG carrier's tank pressure controls, BOG management system or safety valves are compromised, the consequences escalate quickly — from overpressure to rupture, explosion and fire. If main engine, steering gear or bow thruster controls are hijacked, collisions or groundings can follow in confined waters or ports. Whatever the final investigation finds, the *Vivit Africa* incident shows that attackers can already reach a ship's safety-critical systems.

2. Operational disruption

Deviations, diversions and inspection stoppages generate extra fuel costs, port charges and schedule losses. Shore-side system paralysis can close terminals and

back up cargo. The DNV incident and Maersk's estimated USD 300 million loss are both cases in point.

3. Third-party liability

Collisions, oil pollution, cargo loss and damage, personal injury, and damage to port facilities — all triggered by a cyber-attack — still fall within traditional P&I liability categories. The cyber cause does not, in itself, change the nature of the liability. It does, however, complicate how incidents occur, are handled and are claimed.

III. Building a Ship-Shore Defence-in-Depth

As threats escalate, regulations shift from guidance to mandate. IMO Resolution MSC.428(98) has long required cyber-risk management in SMS, with compliance due from the first annual DOC audit on or after 2021. The IMO issued updated maritime cyber risk management guidelines in 2025. On the newbuilding side, IACS Unified Requirements UR E26 (Cyber Resilience of Ships) and UR E27 (Cyber Resilience of On-board Systems and Equipment) are mandatory for ships contracted on or after 1 July 2024.

For shipping companies, practical measures fall into five areas:

1. Embed cyber risk in the SMS

Cyber risk is not just the IT department's problem — it is a part of the SMS. A designated person should lead, supported by shore-based IT and cyber teams, with the master's reporting lines clearly defined. Start with an onboard IT/OT asset inventory and risk register, classifying each system — bridge navigation, dynamic positioning, safety systems, propulsion and power generation, communications, cargo control, alarms and monitoring.

Industry practice groups systems into three categories by failure consequence: Category III (highest — navigation, DP, safety, propulsion); Category II (communications, cargo control, alarms, monitoring); Category I (administrative and office systems). Allocate protection resources accordingly. Newbuilds should also verify compliance with IACS UR E26/E27.

2. Strengthen ship-shore technical defence

Network segmentation comes first. OT networks on the bridge and in the engine control room must be physically or logically isolated from crew Wi-Fi and office networks, with firewalls and intrusion detection between critical systems. On

some larger vessels, navigation, propulsion and steering share one network behind a single firewall — breach that boundary and everything is exposed.

Other essentials: individually assigned system accounts with regular password rotation; remote maintenance connections using multi-factor authentication, enabled only for limited windows and closed immediately after use; special attention to satcom terminals and VSAT management ports — well-known weak points; a patch-management plan aligned with vessel operating schedules; up-to-date antivirus; and offline backups of ECDIS routes and configurations, control-system software and critical files, with recoverability tested regularly.

3. Control changes and third-party access

Many intrusions enter through legitimate routes — a vendor's maintenance laptop, a casually inserted USB drive, a remote-access account left permanently open. Follow a formal change-management process: every software installation, configuration change and hardware replacement needs a request, assessment, approval and record. External USB drives and laptops must be scanned before boarding; connection to critical networks requires specific authorisation; and each remote-access session by a service provider should be individually approved and fully logged.

4. Consider human factors

Phishing remains one of the most common intrusion vectors. Train by role and keep attendance records. General crew: spot phishing emails, manage passwords, and handle removable media correctly. Deck officers and engineers: recognise OT system anomalies and execute manual backup procedures. Shore staff: prevent business email compromise and other email fraud.

Beyond training, run regular practical exercises, activating alternative communication channels if ECDIS fails or ship-shore links go down, and taking manual control when engine or steering controls behave abnormally. Include these in the annual drill programme alongside fire and abandon-ship exercises.

5. Prepare an emergency response plan

Every ship needs a concise, workable cyber-incident response plan built around six steps: identify, isolate, report, respond, recover and review.

If crew spot abnormal pop-ups, encrypted files or lost system control, they should immediately disconnect and isolate the affected device and stop using removable media. The master must promptly report the incident to the designated

shore-based cyber contact, with evidence such as photographs. The shore team responds based on incident type and severity, covering sensitive data, computer systems, ship communications and third-party OT applications like ECDIS. Logs, emails and other evidence must be preserved for forensics.

During recovery: collect evidence before reinstalling systems; change all passwords after reinstallation; apply patches before bringing systems back online. Then conduct a post-incident review and update the plan. A standard cyber-incident reporting form should record time, vessel position, affected systems, severity and measures taken, ensuring consistent, well-documented reports to the company, flag State, port State and insurer.

IV. Conclusion

From Maersk's USD 300 million loss in 2017 to an LNG carrier forced off course by suspected cyber interference in 2026, the threat has escalated dramatically in under a decade, from low-level data theft to sophisticated, targeted attacks that manipulate critical navigation and propulsion equipment.

Ships at sea are not immune. Long communication links, ageing industrial control systems, and varying, and frequently rotating cyber awareness among crews make shipboard cyberspace vulnerable, and increasingly attractive to APT groups and professional hacking gangs.

For any integrated ship-shore management system, embedding cyber security fully into corporate safety governance, with responsibilities assigned to positions, rules applied to individuals, and drills run as routine, is no longer optional. It is a baseline requirement that bears on operational continuity, asset security and compliance.

For more information, please contact Managers of the Association.