CYDOME

Guardians of the cybersea

CYDOME RESEARCH

MARITIME CYBER TRENDS

What Shipping Executives Need To Know For 2026

EXECUTIVE SUMMARY

$10M

The average maritime ransomware incident exceeds **$10M** in direct and indirect damages.

150%

150% increase in maritime OT cyber incidents, **87%** of incidens are ransomware.

15 MIN

New vulnerabilities are hacked **within 15 minutes** of publication (down from 5 days in 2024) while the average **time-to-patch remains 15-30** days for critical vulnerabilities.

1000

1,000 GPS spoofing incidents each day impacting 40,000 vessels.

800%

Attacks on routers, firewalls, VPNs and other edge devices **increased by 800%** in 2025.

52/day

50,000 new vulnerabilities published in 2025, **52 critical or high vulnerabilities added each day.**

AGENDA

1
- **The AI Impact on Maritime**
- Perfect Phishing and Vishing at scale
- Synthetic identities
- Warp-speed hacking

2
- **Maritime-Specific Threats in 2025**
- GPS/GNSS Spoofing
- Mass exploits of vulnerabilities in maritime devices: VSAT, Broadside, Metis
- Cryptomining

3
- **Attack Vectors and Vulnerabilities Trends**
- Secure identities beyond MFA
- The social engineering breach: stolen credentials surge
- Firewalls are not enough – edge device crisis
- The visibility crisis: from blind spots to operational shutdown

4 **OT Attacks and Protection**

5 **Business Impact: The Price of Invisible Risks**

6 **Comparing to Our Previous Year's Report**

ABOUT CYDOME

Cydome's class-certified cybersecurity solutions and services are specifically designed for the needs of maritime environments.

AI impact

In 2025 **AI radicalized** whole verticals, changing the paradigm of how businesses run their operations.

It also changed the paradigm of what it takes to be a hacker. For example, in January 2026, **AI autonomously discovered 12 zero-day** vulnerabilities in SSL, one of the most heavily scrutinized codebases in history - including one that went **undetected for 15 years!**

No wonder that **87% of organizations** view AI-related vulnerabilities as the fastest-growing cyber risk of 2025

> In 2025 we were surprised by the revolutionary speed of expansion of AI, from generative models to multi-modal AI and agentic AI, and now even physical AI. This is also seen in the maritime industries: autonomous navigation, optimal fleet operations, condition-based maintenance and others.
>
> Protecting AI-related assets must be a top priority for shipping companies in 2026 as AI is constantly expanding its capabilities and applicable fields.

Mr. Tetsuji Madarame, Former Principal Fellow, DX, NYK

> Shipping companies are deploying AI faster than they are defining cyber accountability. In 2026, the question after an incident won't be 'Was the AI wrong?' but 'Why was it trusted?

KATERINA RAPTAKI, Digital Transformation, Cyber Security and e-Governance specialist, Navios Group

AI impact for maritime : rise of the perfect phishing

2025 was the year of flawless deception in any language.
83% of phishing emails now use AI, and 75% used polymorphic features.

The impact:

Universal native fluency without broken grammar impact trust: Generative AI creates flawless, context-aware, and personalized communications without grammatical errors that stand out, resulting in a perfectly convincing communication.

Diversity: Attackers can now target multi-national crews in their own mother tongues, building immediate trust.

> In 2026, the most significant cybersecurity risk will come from inside the perimeter. As organizations become more digitally integrated, insider risk-whether malicious, compromised, or accidental-will be one of the hardest challenges to detect and manage. My focus for the coming year is on strengthening detection capabilities across the entire fleet, ensuring consistent visibility, behavioral monitoring, and rapid response wherever systems operate. Resilience will increasingly depend on how well we detect subtle signals early, not just how well we defend the edge.

Øystein Brekke-Sanderud, Head of Maritime OT/ICS Security, NORMA Cyber

Agentic Identity Fraud at Scale

- **The Vishing Tipping Point:** Attackers use commoditized AI to clone voices, launching automated "Vishing" calls that mimic trusted authorities such as IT support and C-level executives, resulting in 1,600% surge in voice phishing (Vishing).

- **Case in point:** The level of deppfake is so good, that with in early 2025, a European energy conglomerate **lost $25 million** when attackers used a deepfake audio clone of the CFO to issue live instructions for an urgent wire transfer. The voice sounded exactly right in pauses, tone, and cadence that the funds were gone within hours.

The Era of The Autonomous Attacker: Explosion of Synthetic Identities

Hyper-Realistic Fake Identities: **AI identity fraud is up 195%** in 2025. AI agents now create synthetic identities that are indistinguishable from human users during verification, easily bypassing “captcha” style tests.

Mass-Scale Orchestration: Cybercrime has been democratized; any individual can now automate thousands of fraudulent requests targeting Port Agents, Bunker Suppliers, and Vessel Officers.

Case study:

social engineering IT teams with deep fakes to gain executive-level access to corporate secrets

Scattered Spider hacking goup (AKA Octo-Tempest and UNC3944) was able to manipulate IT teams to gain access, deploy ransomware and extort an alleged $15 million USD from the likes of Ceaser’s Palace in Las Vegas.

One of its attacks was on a logistics company. After failing to gain direct access to an Oracle system (thanks to MFA protection), they managed to social engineer the IT team to provide access to the company’s CFO account. With that, they were able to move laterally within the network using single-sign-on (SSO), eventually compromising systems such as the company’s Snowflake data repository. Only 62 hours after the intrusion, the security team was able to log the intruders out .

Warp Speed Hacking

Using AI, attacks now move at "Machine Speed": **50%-60% of all new vulnerabilities are weaponized within 48 hours of disclosure** (Time-to-Exploit), and attackers begin to scan for new vulnerabilities **within 15 minutes** of the CVE publication. For comparison, TTE (Time-to-Exploit) was 63 days in 2018 and 5 days in 2024, and the avergae time to patch (MTTP) remains 15-30 days for critical vulnerabilities!
With almost 50,000 new vulnerabilities published in 2025, and **52 new critical or high vulnerabiliies published every day**, this mandates the use of **automated patch management** or virtual patching.

- AI models also got much better at identifying vulnerabilities:
  - In early 2026, an AI model found 12 new "zero-day" bugs in OpenSSL, one of the most scrutinized software library ever, including a bug that existed unnoticed for 15 years!
  - When Claude Opus 4.6 model was released in January 2026, it found (autonomously) 500 new high-severity vulnerabilities, including exploits in highly popular libraries.

GNSS and AIS integrity has shifted from a safety concern to a governance issue. In 2026, the priority for shipping companies is to ensure positioning data can be trusted and explained–because it now underpins safety and regulatory requirements, sanctions-related due diligence, insurance response, and reputational risk, not just navigation

Makiko Tani, ClassNK Cybersecurity Team Deputy Manager

GPS/GNSS Spoofing and Jamming

GPS interferences are now a systemic global risk, not a regional one. Incidents in 2025 have shown that GPS spoofing is also a physical safety threat, not just something requiring reporting and some manual navigational skills:

- About **1,000 GPS disruption incidents are observed EVERY DAY**, with more than 40,000 vessels impacted.
- The threat also became a major concern after two severe incidents:
  - In May 2025, containership MSC Antonia was grounded as it ran ashore near Jeddah due to GPS spoofing causing it to deviate from its intended path
  - In June 2025, two oil tankers collided in the Gulf, apparently setting one of them on fire. The cause is suspected to be a navigational error due to GPS spoofing.

In a recent study, 85% of respondents experienced issues with GNSS receivers, and 14% reported that the signal disruptions led the crews and vessels into unsafe or illegal situations.
A third of the respondents reported that they are not confident that their systems could easily detect GNSS and AIS spoofing.

> The number of cyberattacks in the maritime industry in 2025 more than doubled compared to 2024 and cybersecurity has evolved from a back-office IT task into a core executive agenda that demands the direct attention of the CEO and the Board of Directors. Leading shipping companies must proactively adopt advanced cybersecurity technologies and transparently share their progress with the industry.

Ryan Son, Managing Director,
Rakuten Symphony Singapore & Korea

Case study:

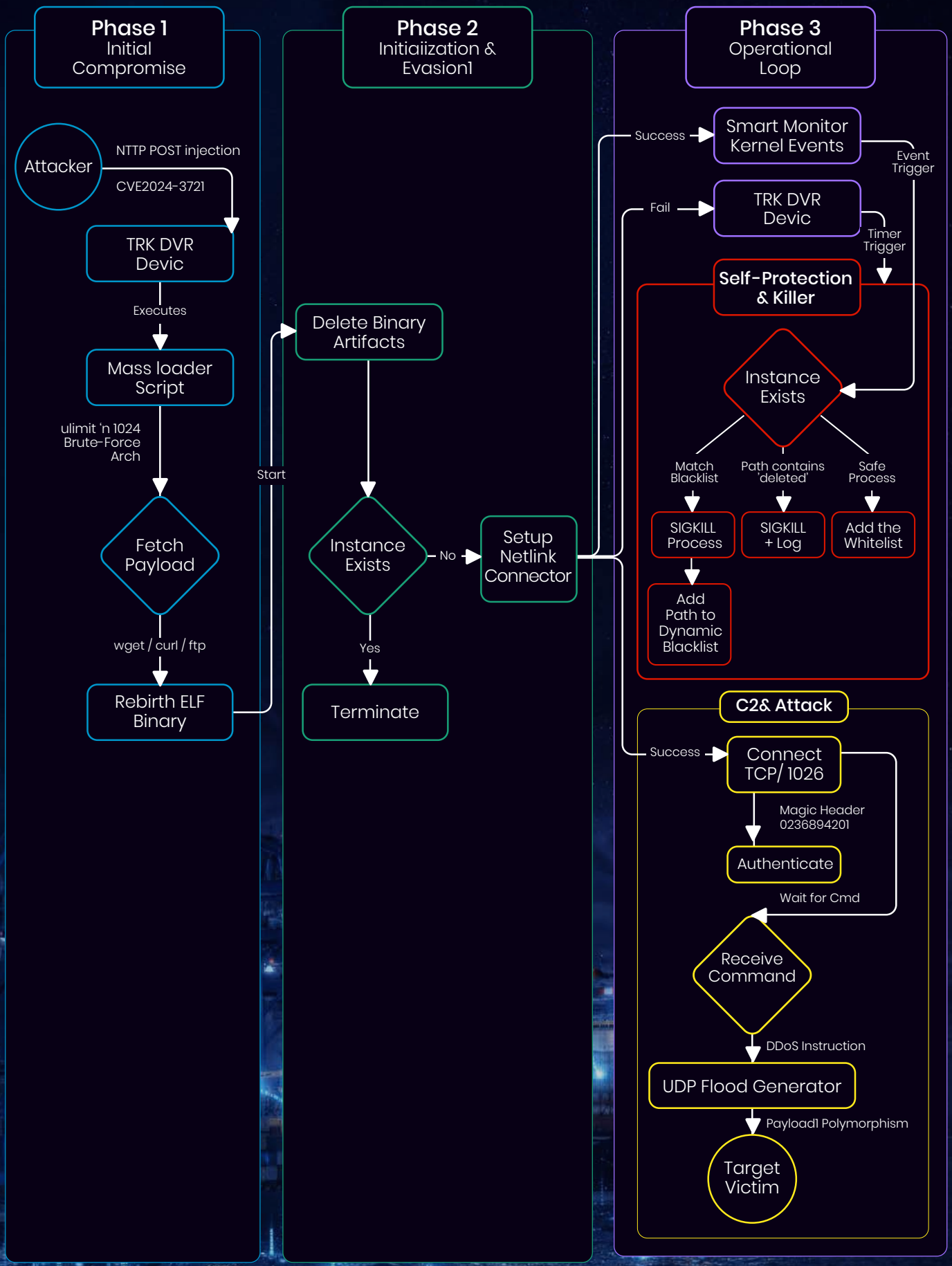
Rise in maritime-specific cyber attacks: the “Broadside” Botnet

In December 2025, Cydome’s cyber research team identified a new, more dangerous variant of the “Mirai” botnet, targeting DVR equipment used in maritime operations.

Unlike previous Mirai variants, Broadside employs special stealth and cyber protection evasion measures, and extends beyond denial-of-service attacks to actively attempt to harvest system credential files.

This attack highlights how even common malware such as botnets, no more than nuisance in many environments, could disrupt operations and cause safety risks in maritime environments where connectivity is a major bottleneck.

Broadside Attack Workflow

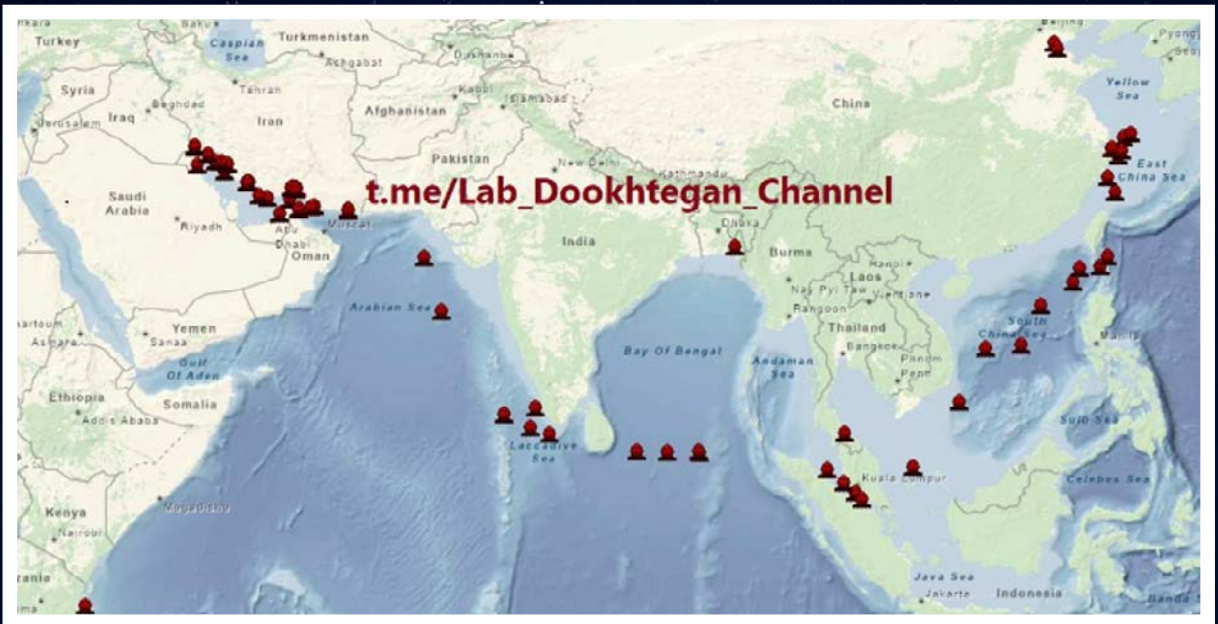


Fleet-Wide Cyber Hacking Of Two Tanker Fleets Highlights Poor VSAT Cyber Posture

In March and August 2025, cyber attacks by hacktivist group "Lab Dookhtegan" ("sealed lips" in Farsi) targeted a fleet of 116 oil tankers belonging to Iranian national companies, disconnecting the ships' VSAT connectivity irreversibly, i.e. requiring technician physical access to resolve.

With the second wave of the attacks in August came the confirmation that the attackers were able to compromise the provider-level infrastructure of Fanava who provided the connectivity to the fleet, thus attacking the entire fleet at once, using destructive techniques and wiping partitions on the VSAT. The attackers also gained control over ship-to-shore VOIP services, further escalating the operational disruption.

While this attack can be attributed to political conflicts in the region, it shows how vulnerable are maritime operations that rely on a single edge device for connectivity.



Ships Are No Longer Isolated: Cryptomining And Bittorrent

Cydome's cyber research team discovered several instances of cryptominers and BitTorrent clients operating on vessels in recent months.

The use of Bittorrent clients on board not only consumes expensive bandwidth, but many Bittorrent clients and downloaded files (including videos) are also prone to malware and cryptomining in disguise of Bittorrent activity: reports show that **43% of torrent software applications contain trojans, and 90% of torrented video game hacks and cheats contain cryptojacking and remote access tools**.

Example: PumaBot, a Go-based Linux botnet, targets embedded IoT devices by brute-forcing SSH credentials, establishing persistence, and executing cryptocurrency mining while using sophisticated evasion tactics.

> In 2026, the fastest and most valuable cybersecurity task for shipping companies is enforcing strict network segmentation between IT and OT systems, combined with MFA and patch discipline.
> It's low-cost, well understood, and immediately reduces the blast radius of both ransomware and remote OT compromise.

Kostas Sakellakos,
IT Manager at NAVARONE SA

> The top priority for 2026 is cyber resilience, and not just cyber protection. Attacks are inevitable and as an incidents analysis indicates are becoming more sophisticated ; the differentiator will be how quickly and safely a shipping company can detect, respond, and continue operations.

Panagiotis Anastasiou, Cyber Security Strategy Leader Bureau Veritas Marine & Offshore

Securing Identities Beyond MFA

When Technical Defenses Meet Human Trust.

Even the strongest Multi-Factor Authentication (MFA) is useless if the human workflow is compromised.

84% of compromised accounts observed in recent breaches already had MFA enabled and 8.3% of digital onboarding processes were flagged as suspicious in 2025 .

Multi-Factor Authentications have been bypassed by technological acumen and through social engineering, and attackers are shifting their focus from “cracking the code” to “manipulating the person”

Examples:

Case studies

KnowBe4

a cyber training company, hired a malicious offender that used a stolen U.S. identity and an AI-enhanced photograph to pass four video interviews and a standard background check. Since the company works remotely, it shipped a company computer to a local address that actually functioned as a "laptop farm" where a facilitator connected the laptop to the internet, allowing the operative (physically located in North Korea or China) to access it via VPN and simulate working from the U.S. The attempt was quickly identified when the SOC team detected unauthorized malware-loading activities and suspicious system configuration changes.

MGM Resort: a common social engineering modus operandi that caused $100M in damages

After reconnaissance on LinkedIn to find names and details of legitimate employees (OSINT), attackers called the IT help desk, impersonating one of these employees, and claimed they were locked out of their account. The help desk reset the credentials and Multi-Factor Authentication (MFA) without rigorous verification, which gave the attackers Super Admin access to the company's IT environments, infecting them with a ransomware. The incident caused MGM to shut down hotel systems, slot machines, and websites for 10 days, costing MGM approximately $100 million in revenue and remediation, as well as a rumored $15M ransom payment.

Examples:

Case studies

Shipping Crew Fraud

in another incident, a fraudster intercepted email communications during a sensitive crew claim and diverted a US$200,000 settlement to its account instead of the family of the deceased crewmember.

Takeaway:

AI identity fraud is highly convincing, even for cyber experts, and attackers identify the human element as the weakest link.

Securing Identities Beyond MFA

Other common MFA bypass technique

Adversary-in-the-Middle (AiTM): the Microsoft 365 Case
A widespread campaign in 2023–2024 targeted over 10,000 organizations using "proxy" phishing sites that simulte a Microsoft 365 login page but in fact steal session cookies. When Microsoft sends the legitimate MFA prompt, the user completes it on the fake site.

MFA prompt bombing
The attackers attempt to login with a stolen password, which sends an MFA prompt to the legitimate user's device. They rely on the user either mistaking it for a genuine prompt or becoming frustrated with continuous prompts, accepting it without thinking too much.

In a notable incident, hackers from the 0ktapus group compromised an **Uber contractor's** login credentials through SMS phishing, then immediately requested a multi-factor authentication (MFA) code. They impersonated an Uber security team member on Slack, convincing the contractor to accept the MFA push notification on their phone.

SIM swapping
Hackers deceive service providers into transferring a target's mobile service to a SIM card under their control, using social engineering. Once transferred, they use the new SIM to receive MFA prompts and gain unauthorized access to accounts.

Takeaway:

Don't rely on passwords as foolproof, minimize access rights and segment networks and systems.

Identity Crisis: Stolen Credentials Surge

- **The 2025 Explosion:** Credential leaks skyrocketed by **160%** this year, fueled by automated AI harvesting and massive third-party data breaches.

- **Bots rise with synthetic identities:** Research finds 82 autonomous agents for every 1 human identity on the internet.

- **The Reuse Trap:** The average user reuses the same password across **four different accounts.** For a Chief Engineer, this means a breach in a personal gaming account can directly compromise the vessel's engine control system.

Falling beyond the Edge: Why Firewalls and VPNs are not enough

- Edge devices remain the primary initial attack vector, and attacks on edge devices (routers, firewalls, VPNs and other remote access tools) are up 800% in 2025

20% of exploits target firewalls and VPNs, 50% of devices with the the most critical vulnerabilities are routers, and 56% of organizations saw a VPN-related attack in the last year, while 46% of vulnerabilities in edge devices were not patched in 2025.

Hackers are bypassing your security by exploiting the security tools themselves, and in 2025 new vulnerabilities were exploited in less than two days while the average fix takes 32 days

Takeaway:

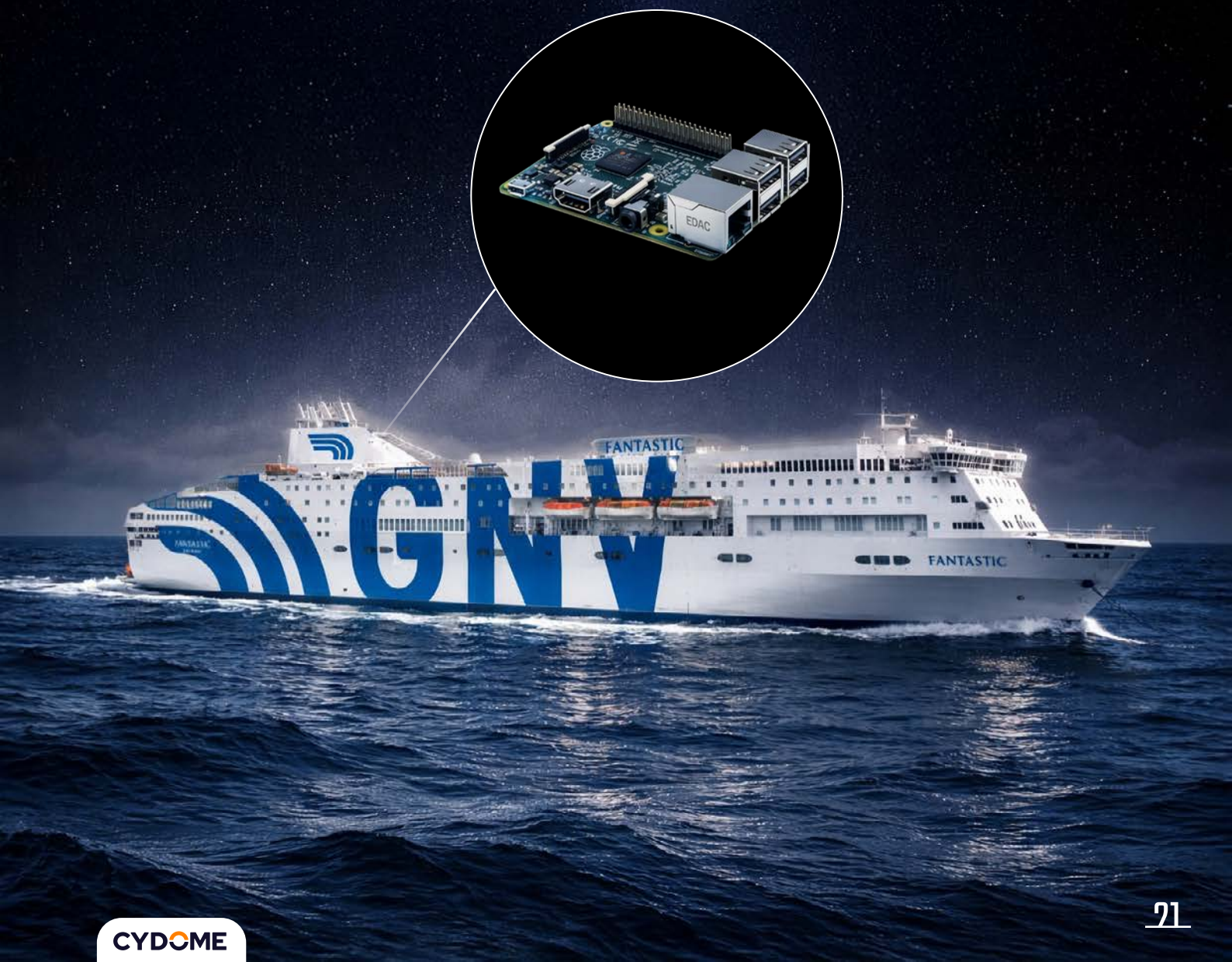
VPNs and firewalls are just one tool, restrict access by role and employ network intrusion monitoring as well.

The Visibility Crisis – Sailing in the Dark

- **"Ghost Asset" Epidemic:** **75% of cybersecurity incidents involved unmanaged "ghost assets"** that security teams cannot see, and 46% of systems with compromised corporate logins were non-managed while only 43% of global organizations use dedicated tools to proactively manage risk across their attack surface.

- This is especially important for ship operations, where crew use unmanaged private devices.

Example: a crew member on board the GNV Fantastic 2,000-passengers ferry attempted to infect the ship's networks with a Remote Access Trojan (RAT) which allows a hacker to gain remote control of a system, using an small, unmanaged compute device (Raspberry Pi).



> In 2025, OT systems became much more connected, while the speed of the regulatory changes preceded the actual technical maturity on board vessels.
> For 2026, shipping companies need to adopt compliance-driven OT cybersecurity, covering not only technology and products but also proper network design and architecture aligned with regulatory and operational requirements.

Despina Panayiotou Theodosiou,
CEO, Tototheo Global

The "Air Gap" is officially dead.

Between high-speed satellite links and the surge in connected OT sensors, your ships are no longer isolated islands but part of a global network where AI is used to scale attacks that were previously too complex for the average hacker. As a result, 22% of organizations suffered an OT/ICS cyber incident in 2025, and **OT incidents now amount to 20% of all reported cyber incidents**, moving from targeting gateways to PLG devices.

Cyber attacks on maritime OT increased by 150%, 87% of them ransomware-driven, and 50% of OT attacks started with unauthorized external access.

The main challenges are:

- **Lack of visibility:** Only 13% of organizations have full OT visibility and can detect an attack on their OT, with 33% having no visibility into OT assets at all. This is especially aggravated in maritime environments as ICS-specific protocols.

- **Third-party access:** Unauthorized external access accounted for 50% of all OT incidents.

- **Aging OT:** More than half of OT is still more than five years old, vulnerable ot exploits and not designed for modern cyber threats and resilience in the age of AI.

- **Specialized systems:** The uniqueness of OT makes it harder to hack, but 49% of OT vulnerabilities are High or Critical.

- **IT/OT convergence:** 75% of all OT attacks begin as IT breaches.

- **Long time to patch:** While IT is patched within 32 days on average, OT takes much longer: 85% of organizations do not conduct regular OT patching and 60% say they only patch under planned maintenance shutdown.

Takeaway:

OT and IT security should be integrated. More CISOs and IT departments take charge for OT security: 50% vs. only 16% 3 years ago.

Case study

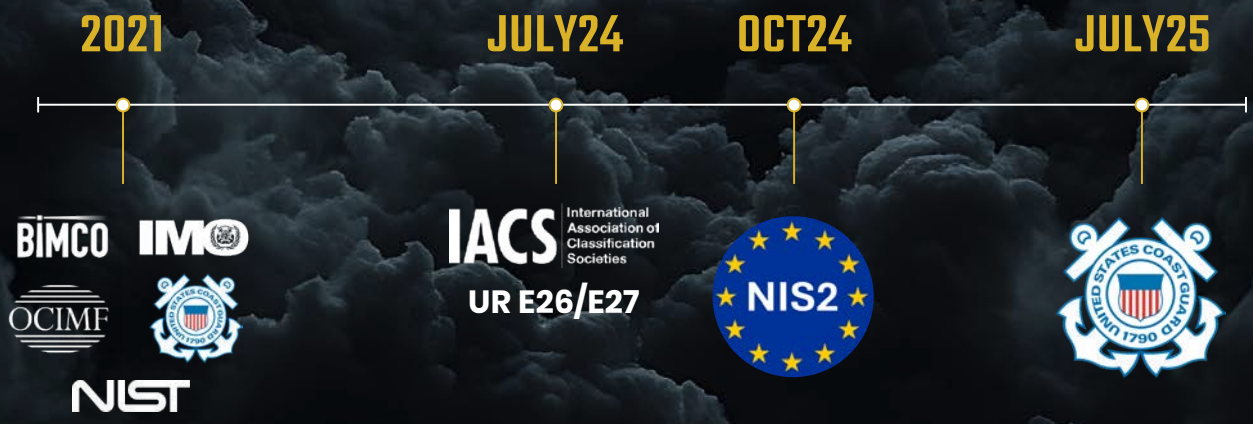
In January 2026 Cydome published a set of vulnerabilities found in two maritime Metis OT monitoring devices by Metis, allowing remote attackers to run unauthorized code with elevated access.

It is time to treat Operational Technology on board a vessel as safety-critical systems, rather than as conventional IT assets. This requires strong network segmentation, unidirectional data flows where feasible, and continuous monitoring tailored to maritime protocols.

Jeroen Pijpker, Researcher at NHL Stenden University

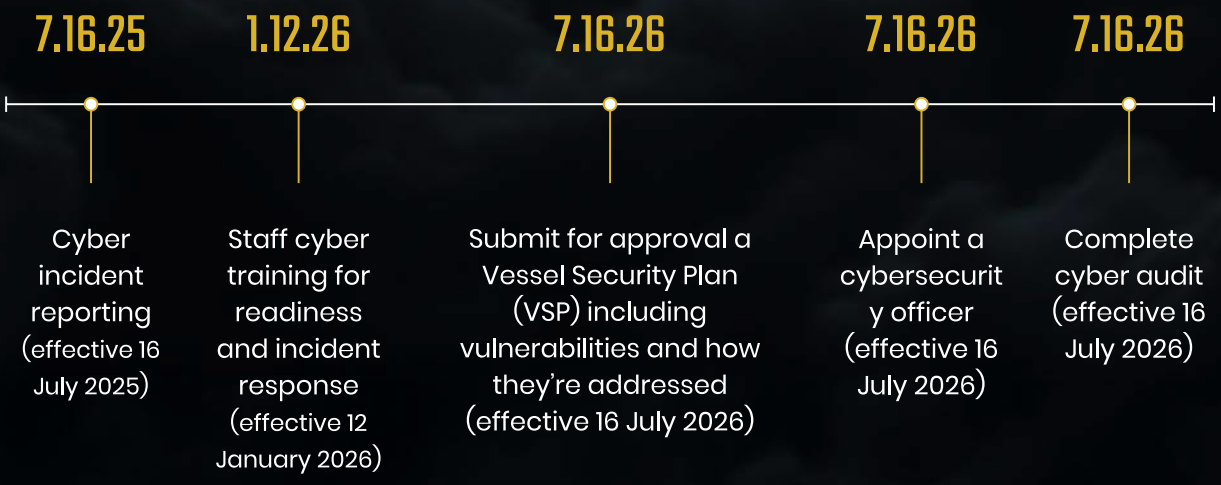
The Regulatory Cyber-Storm

2024-2025 have seen a dramatic change in the regulatory landscape for maritime cybersecurity. IMO, IACS E26/E27, NIS2 and the U.S. Coast Guard regulations are the most prominent requirements, all embracing NIST risk management approach.



In 2025 the new U.S. Coast Guard requirements came into effect based on the following timeline:

- 16 July 2025: Mandatory cyber incident reporting
- 12 January 2026: Mandatory crew cyber awareness training (U.S. vessels)
- 16 July 2027: Submit a Vessel Security Plan, appoint a cybersecurity officer and complete a cyber audit



Business Impact: The Price of Not Doing

> In 2025, maritime cyber risk made it clear that resilience depends on trusted collaboration. Threat actors are moving faster across IT and OT environments, and the organizations that succeed are those pairing qualified service providers with real-time, sector-specific threat intelligence. Information sharing across the maritime ecosystem is no longer optional. It is a force multiplier for operational continuity and safety.

Christy Coffey, VP Operations, Maritime Transportation System ISAC

Business Impact of Cybersecurity

Cybersecurity incidents cause multiple damages, costing on average $4.5 million per incident - a slight decrease from 2024.
A Trend Micro™ survey from 2025 identified the top cyber incident impact factors:

42% Operational continuity	**39%** Market competitiveness	**39%** Customer trust/ brand reputation
39% Supplier relationships	**38%** Employee productivity	**38%** Financial performance

> in 2026, the focus shifts from digitalization to the radical restructuring of business models through AI.

Theofano Somaripa,
Group CIO Newport S.A.

Comparing to Our Previous Year's Report

What has changed from our lat year's report?

AI became ubiquitous even in shipping, but also reaching "production-grade" for hackers.

Ransomware is still the top cyber risk for shipping companies.

While in 2024-5 **unpatched vulnerabilities** were the main attack vector, in 2025-6 exploit of **valid (stolen) credentials** becomes dominant as well.

OT protection is still largely neglected, but several incidents in 2025 brought awareness and we start to see maritime companies adopting stricter OT controls and protection.

Top exploits remain network edge devices: routers, Firewalls, VPNs and remote-connection tools.

> Having battled years of increased uncertainty, disruption is top of mind for the shipping industry. People are acutely aware that supply chains and operations are exposed, and there has never been more need to plug gaps to ensure business can carry on as seamlessly as possible.

Tomer Raanan, Maritime Risk Analyst, Lloyd's List Intelligence

> Cybersecurity protects our people, our reputation, and our ability to deliver reliable service-for every system and for every voyage.

Michalis Michaloliakos PhD , MSc,
Group Head of ICT & Cyber Security TMS Group

CYDOME
Guardians of the cybersea

Follow us on LinkedIn to get the latest updates on maritime cybersecurity

Contact us to discuss your cybersecurity needs:
info@cydome.io

Together, we make maritime travel safer.