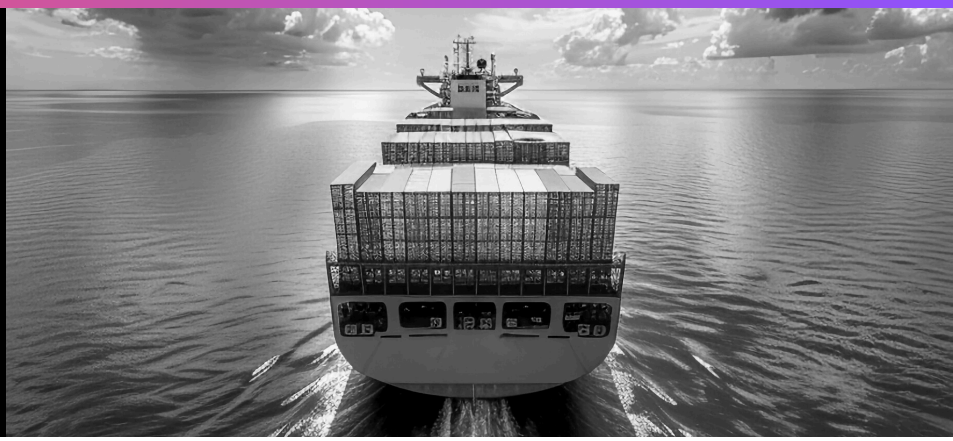
GAPS IN MARITME CYBERSECURITY



Date of Submission: Feb 9, 2026

Author: Nitesh Soni (Head of OT)

Research: Shreya Gujral (Analyst)

Abstract

As the maritime industry moves faster toward using digital tools, cybersecurity has become a key factor in keeping operations safe and reliable, not just a technical issue. The convergence of legacy OT systems, modern IT infrastructure, and IoT-driven connectivity has made the industry more vulnerable to cyberattacks.

This newsletter looks at recent studies, rules, and actual incidents to highlight major cybersecurity weaknesses in maritime operations. These include outdated systems that aren't updated, unsafe communication methods, unclear leadership, and poor sharing of threat information. It also provides clear, research-backed advice on improving cyber safety through better rules, training for staff, stronger leadership, and safely using new technologies.

The aim is to help industry players move from just responding to cyber risks to creating a stronger, more prepared cybersecurity culture across the whole industry.

Table of Content

Introduction

The maritime industry, a backbone of global trade accounting for over 80% of international cargo by volume, has increasingly embraced digital transformation to enhance efficiency, automation, and connectivity. Modern vessels rely on integrated navigation, propulsion control, cargo management systems, and a growing array of IoT-enabled sensors, while port operations leverage advanced terminal operating systems and cloud-based logistics platforms. While these technological advancements improve operational efficiency, they simultaneously expand the attack surface, exposing both vessels and ports to sophisticated cyber threats.

Cybersecurity has become a critical component of maritime safety and resilience. Historically, the sector prioritized physical safety and mechanical reliability, often treating cyber risk as secondary. However, high-profile incidents such as the 2017 NotPetya attack on Maersk, which disrupted container operations worldwide, and more recent ransomware attacks on port terminals and shipping lines have highlighted the tangible operational and financial risks associated with cyber vulnerabilities.

The objective of this paper is to provide a comprehensive analysis of maritime cybersecurity gaps and propose actionable strategies to bridge these deficiencies. Building upon the MDPI 2024 systematic review and recent industry reports, the research explores the following key areas: the state of maritime digital systems, common cybersecurity vulnerabilities, incident trends and financial impacts, existing regulatory frameworks, and best practices for risk mitigation.

1. Research Scope and Purpose

This study focuses on cybersecurity challenges across three primary domains: vessel onboard systems (OT), shipboard and shore-based IT, and communication networks connecting vessels, ports, and third-party service providers.

It aims to synthesize academic research and industry data to identify recurring vulnerabilities and provide a roadmap for maritime stakeholders including shipowners, operators, classification societies, port authorities, and vendors to enhance cyber resilience.

The purpose is not only to document existing challenges but also to recommend practical, evidence-based strategies that can be implemented across the sector.

2. Background & Literature Review

2.1 Maritime Digital Systems: OT, IT, and IoT Integration

Modern maritime operations depend on a mix of different technologies working together. These include Operational Technology (OT), Information Technology (IT), and Internet of Things (IoT) devices. OT systems on ships include tools like Electronic Chart Display and Information Systems (ECDIS), Integrated Navigation Systems (INS), engine controls, and cargo handling systems. These systems were built mainly to help with daily ship operations and not for protecting against cyber attacks, making them easy targets for hackers. IT systems on ships handle administrative tasks, manage logistics through the cloud, and support communication between crew members. IoT devices such as environmental sensors, ballast monitoring equipment, and container tracking tools are becoming more common and are linked to both OT and IT networks, opening up new ways for cyber attacks (MDPI, 2024).

The convergence of OT, IT, and IoT in maritime operations presents unique challenges. OT systems are often old and use special protocols that aren’t easy to update with security fixes. IT systems are usually more up-to-date but are connected to OT networks through gateways that may not be secure enough. IoT devices, used to improve operations, might not follow standard security rules, putting sensitive data about ships and ports at risk.

2.2 Notable Maritime Cybersecurity Incidents

Several incidents underscore the sector's vulnerability:

- **CMA CGM Ransomware (2020)**

  What happened:
  CMA CGM revealed a cyber attack that stopped booking and documentation systems around the world.
  The attack was caused by ransomware from a group called "Ragnar Locker."

  Operational impact:
  Customers couldn't track their shipments or get customs documents for a week.
  Agents had to re-enter data by hand.

  Lesson learned:
  Being open and honest helps build trust.
  By telling customers what happened and working with authorities, CMA CGM prevented worry and avoided legal problems.

- **Iranian GPS Spoofing and AIS Manipulation (2019)**

  What happened:
  Many commercial ships in the Persian Gulf showed GPS locations that were far inside land areas.
  Experts think that people working for a government were checking electronic warfare tools.

  Operational impact:
  1. Ship captains stopped trusting their electronic navigation tools and started using what they could see and basic guessing methods.
  2. Insurance costs for the area went up quickly for a short time.

  Lesson learned:
  Cyber risks aren't just about computers — they can also affect how ships navigate.
  Systems like ECDIS and AIS should not take the place of looking out the window or checking with radar.

- **Port of Antwerp - Drug Cartel Hack (2011-2013)**

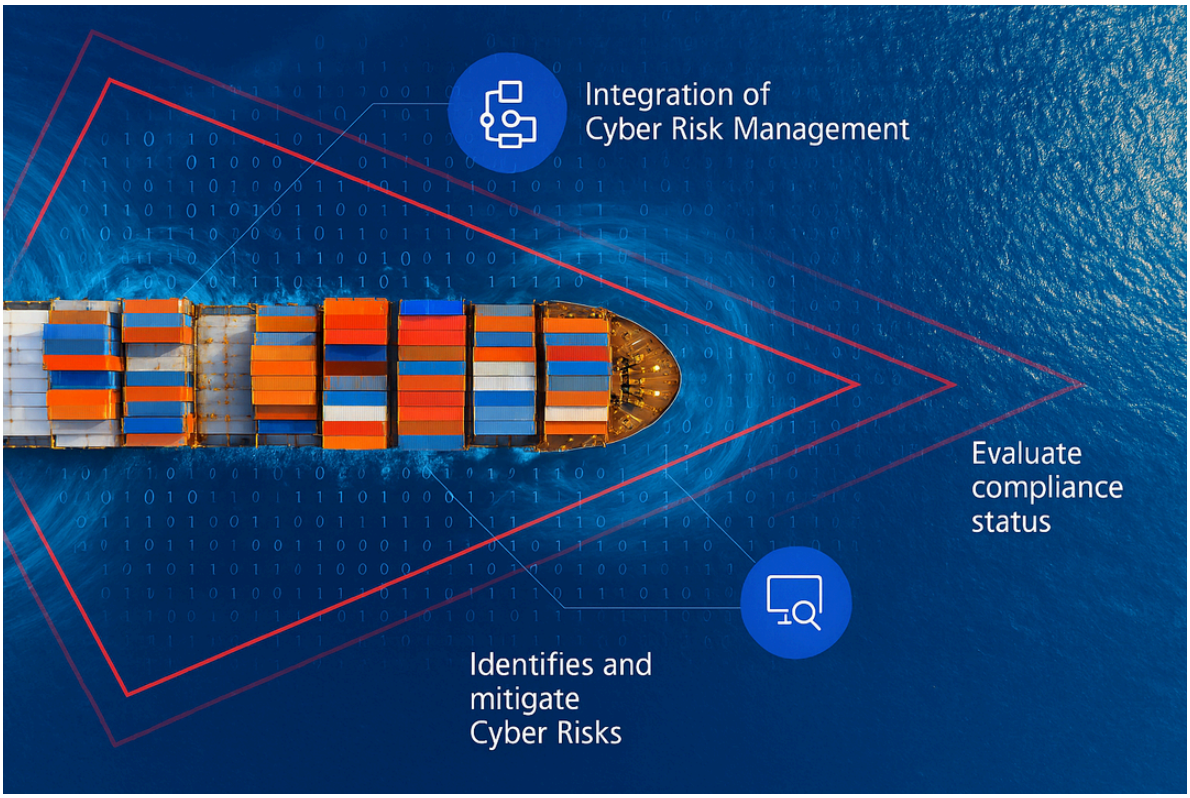
  What happened:
  1. A group of drug dealers in Europe paid hackers to sneak into container terminals in Antwerp.
  2. The hackers changed information about the cargo to hide containers that had illegal drugs.

  Operational impact:
  For two years, the criminals took the containers before the real owners came to get them.
  When the ports noticed some containers were missing, police found out about the theft.

Lesson learned:
Cybercrime can work with traditional smuggling.
Port security needs to use both digital and physical checks to stay safe.

2.3 Regulatory Landscape

Research and reports from the academic and industry sectors have looked at maritime cybersecurity from many angles:



- **IMO Guidelines (2017, 2021):** These suggest adding cyber risk management to the International Safety Management (ISM) Code, offering a way to find, evaluate, and reduce cyber risks on ships.

- **BIMCO Cybersecurity Guidelines:** These recommend including cyber risk management in contracts, risk management practices, and operational procedures (BIMCO, 2021–2023).

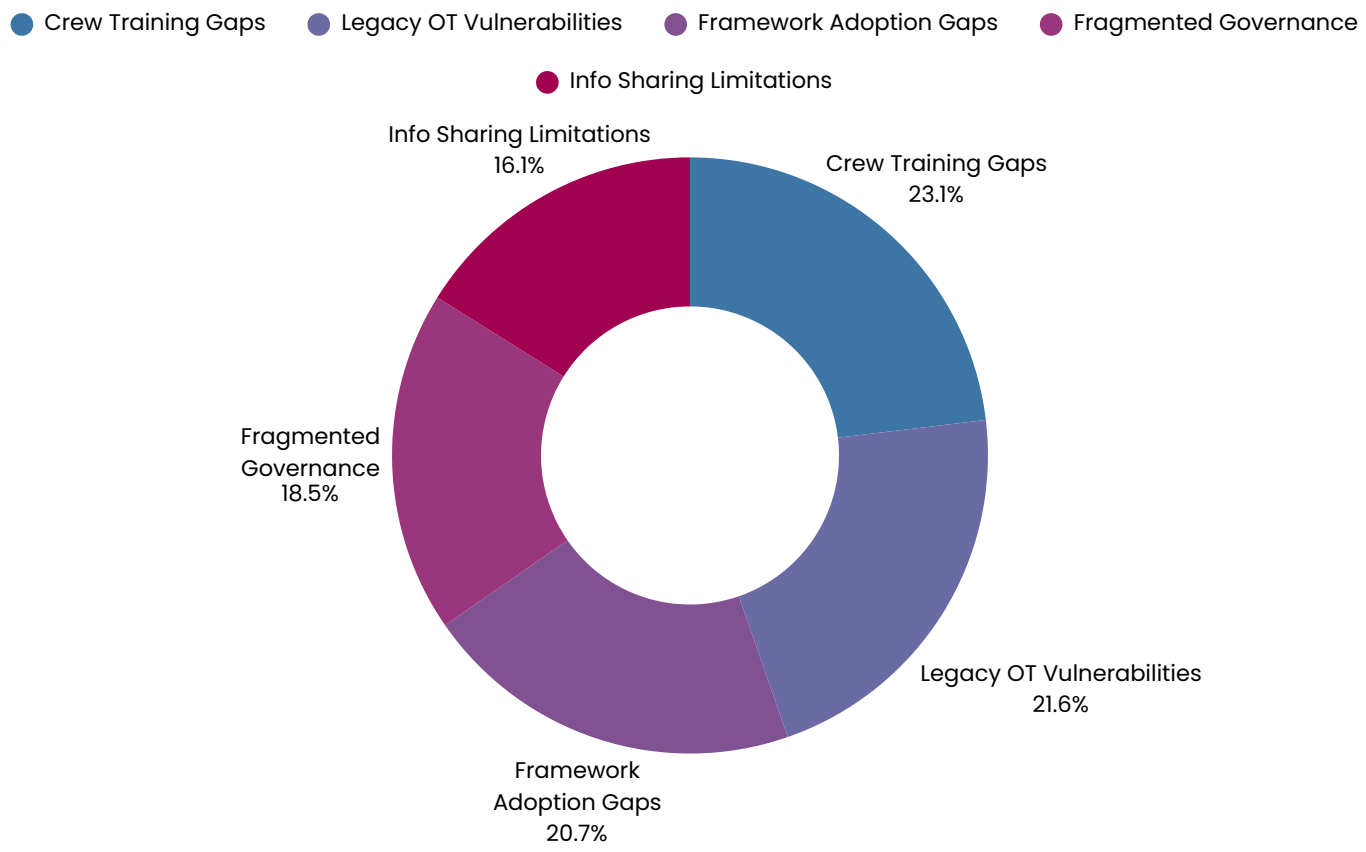
- **ENISA Threat Landscape Reports:** These analyze the ways cyber threats can strike and offer specific cybersecurity tips for maritime operators (ENISA, 2022).

- **Classification Societies:** DNV, Lloyd's Register, and ABS offer advice on cyber risk assessments, vessel audits, and compliance checks. These often use ISO/IEC 27001 and IEC 62443 standards.

- **Systematic Review Findings (MDPI, 2024):** The review highlights common issues such as the integration of OT and IT systems, lack of crew awareness about cyber threats, gaps in regulations, and limited sharing of threat information. It stresses the need for a

comprehensive, multi-stakeholder approach to managing cyber risks.

2.4 Cybersecurity Challenges Highlighted



Key gaps identified include:

- Legacy OT systems with limited patching capability.
- Fragmented governance and inconsistent regulatory enforcement.
- Insufficient crew training and awareness.
- Vulnerabilities in satellite communications (AIS, VSAT) and ECDIS systems.
- Limited information sharing across the maritime ecosystem.
- Inconsistent adoption of standardized frameworks and industry best practices (MDPI, 2024; ENISA, 2022; DNV, 2023).

3. Key Cybersecurity Challenges in the Maritime Sector

3.1 Legacy Systems and Unpatched OT Vulnerabilities

Many ships still use old operational technology (OT) systems that were made before cybersecurity was a big concern. These systems, like engine control units, ballast water management systems, and ECDIS, often run outdated software with security flaws that haven't been fixed.

Because these systems are old, they are easy targets for hackers who know about the weaknesses. Sometimes, it's hard to update them because of how important they are for ship operations. This means ships can be attacked for a long time without proper protection (MDPI, 2024).

3.2 Fragmented Cybersecurity Standards and Governance

The maritime industry lacks a unified approach to cybersecurity. Even though there are guidelines like the IMO guidelines, the ISM Code, and MSC.428(98), they aren't used the same everywhere. Many companies only do what's required to stay compliant, not much more. Control over cybersecurity is shared between different groups like ship owners, charterers, port authorities, flag states, and classification societies.

This leads to confusion about who is responsible and inconsistent enforcement. There's no common standard or certification for ships and ports, so security levels can vary a lot. As a result, the industry tends to respond to problems after they happen, has uneven awareness of risks along the supply chain, and is more vulnerable to major disruptions on important trade routes.

3.3 Crew Awareness and Social Engineering Risks

Human mistakes are one of the main causes of cyber incidents at sea. Many crew members and workers on land don’t have proper cybersecurity training, making them easy targets for phishing, targeted phishing, and other social engineering attacks.

A DNV report (2023) found that fewer than 30% of crew members could correctly identify phishing emails or follow secure login practices. This shows the importance of ongoing training and awareness programs.

3.4 Insecure Satellite and Communication Links

Satellite communication systems, like AIS, VSAT, and other ways to connect ships to land, are often not protected well.

These systems are key for navigation, managing cargo, and coordinating operations, so they

are especially vulnerable to attacks like eavesdropping, fake signals, and jamming. Poor security in ECDIS systems also makes these risks worse (ENISA, 2022).

3.5 Limited Incident Response and Threat Intelligence Sharing

The maritime industry doesn’t have a central place where companies can share information about cyber threats.

This leads to the same attacks happening over and over again. Legal limits, competition, and different rules across the industry stop companies from sharing data about incidents. As a result, lessons aren't shared properly, and attacks keep happening (MDPI, 2024).

3.7 Supply Chain and Third-Party Risks

Companies that provide services or products to maritime operators, like software developers, satellite providers, and port logistics, can create new security risks.

These companies often have different security policies, making them weak points in the overall system. Many contracts don’t include strong cybersecurity requirements, and there’s no regular checking or assessment of their security.

3.8 Emerging Technology Risk

New technologies like digital twins, autonomous ships, and IoT-enabled cargo monitoring are being used more in the maritime industry.

These tools rely on cloud connections and remote access, which can expand the areas where hackers can attack. Without strong cybersecurity built into these systems from the beginning, they could make the industry more vulnerable to cyber threats.

4. Solutions

The cybersecurity challenges in the maritime industry are complex and require a comprehensive approach that combines technology, rules, human behavior, and international teamwork. The following sections provide specific solutions for each of the identified challenges and areas needing improvement.

4.1 Modernizing Legacy Systems and Securing OT Environments

To address vulnerabilities in legacy operational technology (OT), progressive system modernization and secure lifecycle management are essential. Ship operators should create

clear plans for fixing software and schedule updates during planned maintenance times to avoid disrupting daily operations (DNV, 2024). For systems that cannot be updated because the vendor no longer supports them, using virtual patches and dividing the network into sections can help protect against risks.

Using firewalls to separate parts of the network, one-way gateways, and OT intrusion detection systems (IDS) can help protect key parts of the ship such as the propulsion system and engine control.

The IEC 62443 standards offer a guide for assessing risks and safely integrating systems. Classification societies such as ABS and Lloyd's Register now offer cybersecurity certifications (like ABS CyberSafety® and LR Cyber Secure) that encourage better practices through recognition and support.

4.2 Establishing Standardized Cybersecurity Frameworks and Compliance

The way forward is alignment, not more isolated rules. Adopting proven frameworks like NIST CSF 2.0, ISO/IEC 27001, and IMO cybersecurity guidelines would give the industry a shared language, clear maturity benchmarks, and measurable controls across fleets, ports, and regions.

This needs to be backed by stronger governance under the IMO, with flag states enforcing cyber requirements through the ISM Code and classification societies providing independent assurance. Introducing a Maritime Cyber Maturity Index would make cyber readiness visible and comparable, while port-level cyber coordinators and expanded IMO audits would improve oversight and information flow.

At a global level, closer coordination between the IMO and classification societies through a common convention, combined with standardized certification for ships and ports and a shared threat-intelligence platform, would shift maritime cybersecurity from fragmented compliance to proactive, prevention-led risk management.

4.3 Enhancing Crew Awareness and Reducing Human-Error Risks

To fight phishing and social engineering attacks, shipping companies should make regular cybersecurity training part of crew training. The STCW should include mandatory lessons on cybersecurity. Practices like simulated phishing, password protection training, and using multiple layers of security can greatly reduce risks from human mistakes.

A study by DNV (2023) found that organizations with regular cybersecurity training saw a **52%**

drop in successful phishing attempts within a year. Training should also include shore-based staff to ensure security across all areas of operations. Working with maritime schools to include cybersecurity in officer training will help create a safer culture long-term.

4.4 Securing Satellite and Communication Infrastructure

Securing maritime communications needs full encryption, strong user identification, and backup connections. Satellite operators should use AES-256 encryption and PKI (Public Key Infrastructure) for data sent through AIS, VSAT, and GMDSS systems (ENISA, 2023).

To deal with spoofing and jamming attacks, ships can use systems that check positions from multiple sources, like combining GNSS with other positioning systems and radar data. ENISA (2022) also recommends using tools that detect sudden changes in AIS data to spot problems. Working with satellite providers to test networks for weaknesses through penetration tests and simulations can help find and fix problems before they are exploited.

4.5 Strengthening Incident Response and Threat Intelligence Sharing

A proactive Maritime Cyber Incident Response Framework (MCIRF) should ensure consistent steps for detecting, reporting, and managing cyber incidents, supported by internal or outsourced SOCs for 24/7 monitoring. Threat-intelligence sharing through bodies like MCERT should become routine, as anonymized incident data helps reveal trends—Norway's MCRC found that participants resolved incidents 40% faster (DNV, 2024). Regular cyber drills within safety management systems, coordinated with flag states and port authorities, further strengthen collective incident response.

4.6 Securing the Supply Chain and Third-Party Ecosystem

Given the high dependency on third-party vendors, shipping companies should adopt Zero Trust Architecture (ZTA) and perform continuous supplier risk assessments. Contracts must require suppliers to follow ISO/IEC 28001 and have annual cybersecurity audits.

To stop infections from removable media, companies should implement policies that control devices, such as only allowing approved USB drives, encrypting removable storage, and keeping records of all data transfers. Using automated endpoint protection tools has reduced malware attacks by up to 70% in some maritime settings.

Additionally, using blockchain to verify the identity of vendors and equipment can help prevent fraud and ensure that software updates are genuine, which lowers the chance of tampering or fake updates.

4.7 Reducing the Expanding Attack Surface and Managing Future Risks

The rapid increase in connected devices on ships and in ports needs better cybersecurity plans. Ships and ports should use tools to find and track all connected devices in real time. AI-powered systems can spot unusual activity in networks, helping to find threats faster and reduce false alarms.

To deal with risks from hybrid warfare and attacks on important systems, governments and industry groups must include cyber resilience in national maritime security plans. The global market for maritime cybersecurity is worth $3.19 billion as of 2024 and is expected to grow to $9.01 billion by 2033 (Grand View Research, 2024), showing how urgent and valuable this is.

Long-term solutions involve better teamwork between the maritime, energy, and aviation sectors to share information and set common standards. Having backup communication systems, using different satellite providers, and using encryption that can resist future quantum computing threats will help protect maritime operations in the future.

5.Conclusion

The maritime industry is at a key point where digital progress meets cyber risks. This study shows that cyber dangers aren't just technical problems but are linked to bigger issues like governance, technology, and human behavior. Old systems, inconsistent standards, and poor training are still holding back the ability to respond well to cyber threats across ships and ports.

To manage these risks, a layered approach with teamwork is needed.
This includes:

- Updating both operational and information technology systems with security in mind from the start.
- Making cybersecurity training and drills a regular part of crew routines.
- Setting common international standards with support from the IMO.
- Sharing real-time threat information across the entire maritime system.
- Using AI and machine learning to identify and respond to threats quickly.

Moving forward, achieving cyber resilience in the maritime industry depends on matching new technology with clear rules and building a global focus on cyber awareness. Through common standards and sharing information across different sectors, the maritime world can protect its digital changes while keeping trade safe, reliable, and efficient.

6. References

- Journal of Marine Science and Engineering, 12(6), 919 - https://www.mdpi.com/2077-1312/12/6/919

- International Maritime Organization (IMO). (2025) - https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/FAL%20related%20non mandatory%20documents/MSC-FAL.1-Circ.3-Rev.3.pdf
- International Maritime Organization (IMO). (2017) - https://www.imo.org/en/ourwork/safety/pages/
- BIMCO et al. (2024) - https://www.bimco.org/media/s4ddrsfe/2024-11-14-guidelines_on_cyber_security-v5-final.pdf
- European Union Agency for Cybersecurity (ENISA). (2022) - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
- DNV. (2024) - https://www.dnv.com/cyber/insights/publications/maritime-cyber-priority-2024/
- Allianz Global Corporate & Specialty (AGCS). (2018) - https://commercial.allianz.com/news-and-insights/expert-risk-articles/shippers-cyber-threat.html
- Grand View Research. (2024) - https://www.grandviewresearch.com/industry-analysis/maritime-cybersecurity-market-report
- Port of Houston Authority. (2021) - https://www.infosecurity-magazine.com/news/port-of-houston-quells-cyberattack/
- Marpoint. (2024) - https://marpoint.gr/blog/2024-a-year-of-rising-tides-in-maritime-cybersecurity/