International Journal of Core Engineering & Management
Volume-6, Issue-11, 2021 ISSN No: 2348-9510

CYBERSECURITY IN THE CRUISE SHIP AND MARINE SHIP INDUSTRY

Udit Patel,
devashishm91@gmail.com

Abstract

Technology in any aspect of vessel and cruise operation is intensive, particularly in digital systems, which makes it prone to cyber threats as organizations adopt networked systems. This paper focuses on cybersecurity in the maritime industry, with particular attention being paid to the issue of the protection of passengers' data and the safety of systems on board ships. The paper categorizes the data often collected on cruise ships, including the users' payment information, health status, and location data, before presenting the many possible threats that data breaches pose to organizations within that high-tech sector. Also, it identifies the company's compliance with international legislation, such as GDPR or Data Privacy Regulation; PCI DSS for securing personal credit card data; and HIPAA for the safe management and sharing of patients' health information. Finally, the paper also covers some recommendations on how passenger information can be protected, including encrypting data, networking segmentation, and training employees to handle the info. When adopting these measures, the maritime sector will be able to reduce cyber-threat risks, protect the passenger's right to privacy, and guarantee the sector's operational security.

Keywords: Maritime cybersecurity, Data privacy, Passenger information protection, Cruise ship data security, GDPR, PCI DSS, Health data security, Network, Cyber threat, Operational resilience

I. INTRODUCTION

The digital embrace has seen a tectonic shift in the maritime and cruise ship industries in recent years. These innovations are shaping maritime operations with advanced navigation systems and sophisticated tools of communications, among many others. Satellite communications, Internet of Things (IoT) devices, and onboard networks have been integral in helping improve operational efficiency, enhance the passenger experience, and support safety in commercial and cruise ships. While these technologies evolve, the industry's reliance on interconnected systems and real-time data exchange continues to increase, and, therefore, the sector remains more vulnerable to cyber threats. Along with this expanding dependence on digital technologies within the maritime and cruise ship sectors, there is also the possibility of rising cyber-attack threats. With growing numbers of systems going digital, the attack surface grows, and cybercriminals have new places to penetrate.

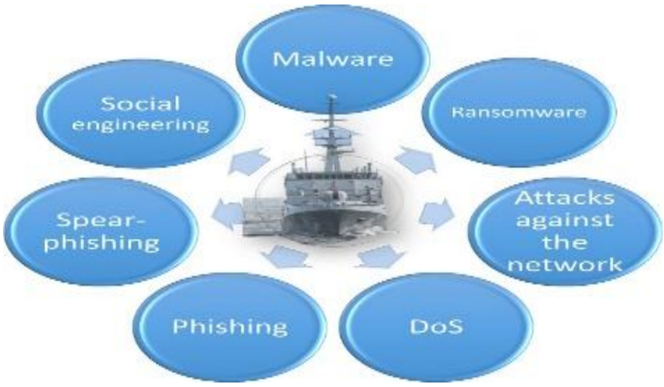


Figure 1 : Maritime cybersecurity: protecting digital seas

II. POTENTIAL CONSEQUENCES OF CYBERSECURITY BREACHES

The cruise industry is a prime target for cyberattacks for various reasons. First of all, its onboard and shore-based network involves many systems that, between themselves and the passengers they store their data on, build a complex analytics ecosystem to ensure navigation and all things that can occur at sea. In addition, human nature leads cybercriminals to believe that these systems handle sensitive information, such as passengers' identification and payment details, rendering them appropriate targets for ransomware attacks, phishing attacks, and data breach breaches. However, such attacks' catastrophic consequences are very high—they can cause severe operational disruption, financial loss, and tarnish the reputation.

The complexity and scale of maritime operations add to the threat of cyberattacks in that 90% of the industry's activities are related to global trade, so it is easy to understand why any problems in the sector have enormous effects on the entire circulation. Maritime and cruise lines become APTs (Advanced persistent threats) targets, often directed by nation-states or organized criminal organizations—the targeted. Cyber-attacks involve compromising critical infrastructure, disrupting operations, and unauthorized access to sensitive data. For example, ransomware can take down port operations, and GPS spoofing could mislead ships and the route t routing into dangerous or pirated waters. Under these dubious developments, the maritime and cruise ship industries must adopt a general approach to cybersecurity as the risk of them keeps rising. To ensure crew and passengers' safety and security, operational technologies (OT), such as navigation, engine control, and safety systems, must be protected. In addition, any sensitive information relating to passenger data and finances must be protected from cyber criminals to enjoy trust and meet international regulations such as the General Data Protection Regulation. Maritime operators can significantly mitigate the cyber security risk for their organization when robust cybersecurity protocols are implemented, including network segmentation, multi-factor authentication, and regular system updates.

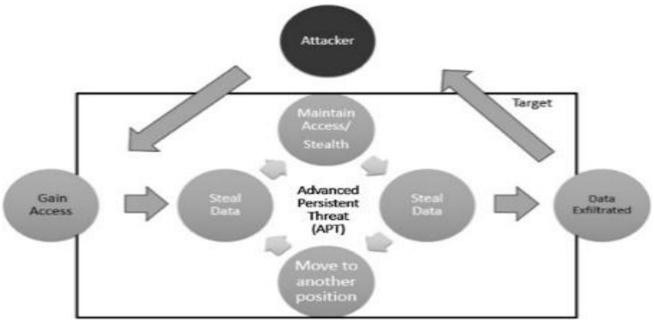


Figure 2: Advanced Persistent Threat - an overview

III. THE IMPORTANCE OF CYBERSECURITY IN THE MARITIME AND CRUISE INDUSTRIES

Due to maritime and cruise operations depending heavily on digital technologies, the demand for cybersecurity operations has also risen significantly across these industries. The integration of technologies improves organizational performance but simultaneously increases the vulnerability of these industries to cyberattacks with potentially serious repercussions. These cyber risks likewise endanger not only business operations but also the safety of passengers and financial solvency (Venizelou, 2018). In this section, we shall look at how technology plays out in the maritime sector, the effects of cyber incidences, and examples of previous cyber experiences that Maritime should learn from to enhance protection.

1. Role of Digital Technologies in Daily Operation

IT solutions play a critical role in day-to-day business operations for maritime and other industries. Inspectors' functions like navigation, communication, engine, and cargo management were now dominated by digital applications that enabled ships and ports to work efficiently and dynamically. Fleet management through the use of these actions has advanced. It provides more frequent monitoring of vessels and their assets, safety, and general efficiency in the supply chain. In addition, passengers riding on a cruise ship will also expect functional wireless signals, digital amusement, and intelligent control of rooms, which adds complexity to the technological frameworks on these ships. Although they make things more efficient, all these advances expand the exposure cybercriminals have to target. They are connected to shore operations, resulting in extensive networks with a single weak point sufficient to compromise essential networks. Maritime cybersecurity needs to be a focal topic of discussion today to ensure the risk of disruption and cyberattacks is minimized (Hayes, 2016). At the same time, firm data, mainly financial information, navigation, and cargo detail data, are protected, given today's increased use of digital platforms in the maritime industry.

2. Potential Effects of Cyber Security Breaches

Maritime and cruise sector security threats can lead to many more problems. The consequence of a successful attack is that the organization's operation is threatened, apart from endangering the lives of crew and passengers. For example, applying pressure to control the direction of the car or ship's navigation can lead to a loss of control over it, leading to collisions or polluting the environment (Gill, 2018). In the cruise industry, breaches could be lethal as they compromise the lives of the passengers, and the malicious actors render lifeboat controls or other means of communication inoperative (Andreadakis & Sloane, 2021). Furthermore, threats to organizations' finances are a real possibility, as cyber losses can be catastrophic. Just one ransomware attack can prevent operations in a seaport; in other words, it may take several days to resume work, resulting in significant disruptions to international trade and vendors and purchasers losing millions of dollars. They have also led to leaking clients' personal information, such as credit card details and patient data. An example of a breach could harm a company's reputation with its customers and almost certainly result in legal action under the GDPR. This is because the operations of maritime businesses and companies have an intricate relationship with each other, hence rendering one sector vulnerable to cyber threats that destabilize others. Carriers, terminals, and logistics companies are potentially exposed; therefore, cybersecurity must be recognized as an issue for the maritime chain.

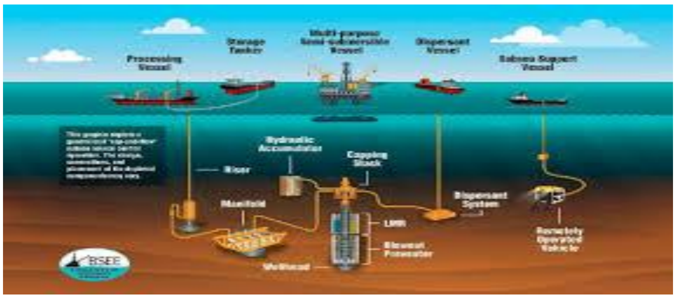


Figure 3: Accidental Spill Mitigation

3. Historical Cases Of Cyber Security In The Maritime Industry And Their Impacts

Some examples of cyber-attacks that have occurred in the recent past are as follows: The maritime industry needs cybersecurity. One of the most famous case reports occurred in 2017 when the Danish global business engaged in shipping and oil and gas, Maersk, was attacked by the NotPetya ransomware. This attack paralyzed Maersk's operations worldwide and its capacity to coordinate shipping solutions and was estimated to have cost the company $300 million. NotPetya attack demonstrated that the maritime industry is underprepared for ransomware attacks if it is an option to have any (Ryan, 2020). This case also emphasized the necessity of having sound IRDR plans. Another real-life example is the 2018 ransomware attack on a port in San Diego, which threw operations into disarray. To prevent the further spread of malware, the systems were disconnected. As much as physical security was not under threat during the attack, operational disruption and financial losses were seen in delays in cargo handling and shipping (Nyati, 2018). They revealed that cruise lines also emerge as ideal targets for cybercriminals. Speaking of ransomware attacks in 2020, one of the biggest cruise operators, Carnival Corporation, suffered through an IT system breach and subsequently disclosed customer and employee data leakage. It was costly as it endangered the business monetarily and exposed the company to lawsuits and potential GDPR fines. These cases show the most routine cyber threats maritime businesses face today and exemplify the importance of systematically approaching cybersecurity. Maritime and cruise industries need to enhance their cybersecurity because they are implementing new technologies that enhance their functionality but also have vulnerabilities. These risks include operational interdependencies, cost implications, and passenger safety, making cybersecurity a critical discipline. Real-life hacker attacks at Maersk and Carnival Corporation are good examples of threats lurking in these industries (Burrell, 2012). If the threats shift, the maritime industry has to put up its guard higher and safeguard its property and the people on board.

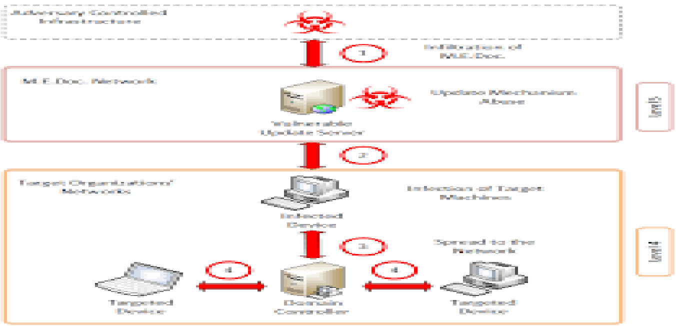


Figure 4: The NotPetya attack process

IV. CRITICAL CYBER THREATS IN THE MARITIME INDUSTRY

The maritime industry is vulnerable to many cyber threats as it relies on digital platforms. These risks can hamper operations, jeopardize information integrity, and incur grave business and image consequences. The following outlines vital cyber threats in the maritime sector:

1. Ransomware Attacks

Ransomware is malware that extorts money by encrypting data while requesting it to be paid, usually in bitcoins. This often penetrates a computer through phishing emails, downloads from unsecured websites, and through unsecured networks. Once a system is penetrated, it becomes straightforward for attackers to deny users access to specific systems or files and thus bring operations to a standstill (Mitnick & Simon, 2009). In the maritime industry, ransomware hits the shipping and port operators, leading to massive losses. One of the biggest is the 2017 NotPetya attack on Maersk, one of the world's biggest shipping companies. The ransomware attacks paralyzed Maersk's business worldwide, leading to a net revenue loss of between $250 and $300m because its IT platforms and all its terminals were shut down.

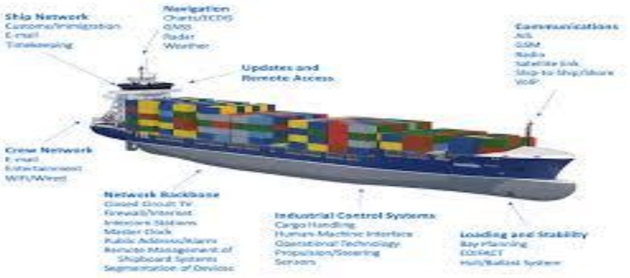


Figure 5: A system of systems: Cooperation on maritime cybersecurity

2. Malware and Viruses

Viruses, Trojans , worms, and any other type of malware can gain access to the order of the maritime system, of course, of the order of the maritime system course, through contaminated USB, contaminated files receive email, among others—these programs email systems, from navigation and engine control to cargo management systems. For instance, pirate malware attacks in a ship's navigation system may tamper with the GPS so that a vessel strays off course. At worst, cyber-threats have been reported to disrupt critical operational systems such as engine control, management, and cargo discharge, resulting in likely outcomes, accidents, or even pollution. Further, lack of or outdated patching implementation on the ship-primarily based programs poses a risk to malware attacks because the hackers could access the programs since they contain previously recognized weak spots.

3. Phishing and Social Engineering

Phishing and social engineering attacks use people's failure, whereby an individual is deceived into parting with important information or getting the attacker into the system. Phishing is usually a bogus email or message that looks genuine, making the victim act like clicking on a dangerous link or opening a bait. In the maritime industry, these attacks are typically aimed at individuals who work directly on operational or financial systems (Berle et al, 2011). For instance, the attackers may masquerade as company managers, executives, or suppliers to make employees let them access essential documents or transfer money to specified accounts. This also stretches to impersonating other trusted sources for hijacking ships' operating systems and exposing them to cyber intrusions.

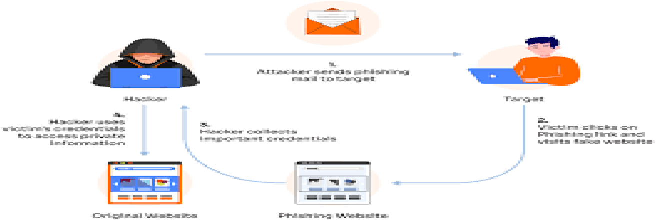

1.
Attacker sends phishing mail to target
Hacker
Target
4.
Hacker uses victim's credentials to access private information
3.
Hacker collects important credentials
2.
Victim clicks on Phishing link and visits fake website
Original Website
Phishing Website

Figure 6: Complete Guide to Phishing: Techniques & Mitigations

4. Supply Chain Attacks

Manufacturers must depend on third-party vendors for feature updates, maintenance, and equipment supplies in maritime operations. This dependency creates weakness because an unscrupulous vendor can introduce malware to the client's systems. A supply chain attack involves penetration of a company's supply network to introduce malware in software updates or hardware gadgets. For example, a firm can receive a payload with malware from a vendor, and subsequently, many ships/ports will be affected, leading to industry-wide disruption. Such attacks are dangerous because many maritime operations are interdependent, and the breach of one vendor can be problematic for many other systems.

5. GPS Spoofing

GPS spoofing is another subcategory of cyberattacks that involves sending fake GPS signals to a vessel's NAV system. This leads to the ship providing wrong positions, resulting in collision or grounding in usually dangerous zones. In 2017, several ships with GPS navigation systems off the coast of the Black Sea were targeted with spoofing attacks in which the GPS screens showed fake locations. They can have very drastic outcomes, particularly in a congested section of approaching sea traffic lanes or near any vulnerable areas. Further, GPS jamming that interferes with signals entirely remains another threat to the industry, specifically for self-directed or partly self-driven vessels.

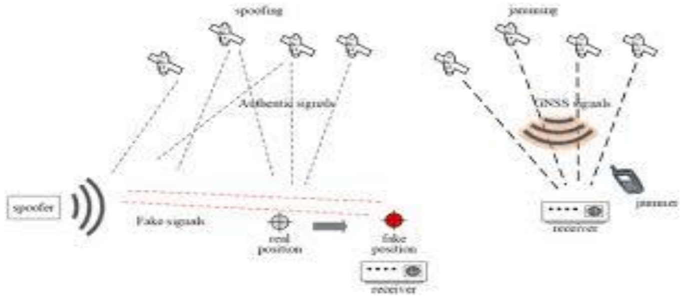


Figure 7: Recent Advances on Jamming and Spoofing Detection in GNSS

6. Attacks on Port Infrastructure

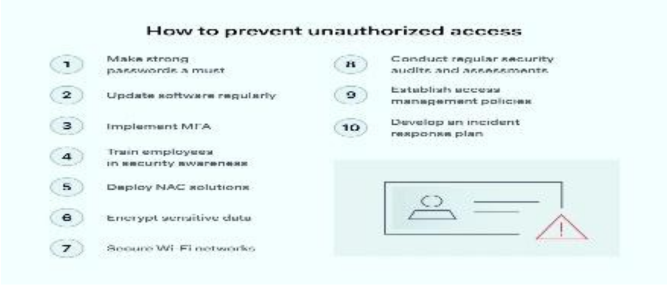
Haven is an essential link in the international logistics chain, where many numbers go through daily. The critical prerequisite is that they rely on digital systems for handling cargo, planning logistics, and communication. The threat of disruptive cyberattacks on port infrastructure successfully could put the global economy under pressure, bring the inter-organizational supply chains to a complete standstill, and jeopardize significant losses. For instance, a ransomware assault on one of the ports' logistic information systems might affect the shipment and handling of goods and inflict commercial and image losses on shippers. Ports remain also vulnerable to physical damage through cyber means, such as damage to auto cranes or interference with a tagging system for cargo.

7. Insider Threats

The unique cyber via risk exists for employees and contractors with IT access to information and systems. In this case, insider threats are employees who may be dissatisfied with their employer or contractors with an evil intention towards the contracts they signed or third parties who may unknowingly have their device or system (Mehan, 2016). For example, the employee of a shipping company who has access to the operational technologies of a particular vessel may leak specific information to rivals or insert viruses into the main ship's systems. In insider threat management, strong control measures, such as the right of entry, screening, and pervasive observation of the employees' behaviour, are used to identify potentially dangerous actions.

8. Data Breaches and Financial Losses

The maritime industry deals with sizeable amounts of data-sensitive information such as cargo manifests, the ships' and consignees' financial transactions, and passenger data. This data is vulnerable to attacks by cybercriminals to defraud or cause a Denial-of-Service attack on the organization. Changing passwords may give unauthorized people access to an organization's data, and money and reputations may be lost due to leaked Restricted data. Further, such data can be sold to third parties on the dark web or to launch other cyberattacks. Depending on the circumstances, the lost data may contain the passenger's identity information, personal/auto/fleet credit card details, and travel schedules, which can be valuable to criminals, particularly in identity theft and fraudulent activities.



How to prevent unauthorized access

1. Make strong passwords a must
2. Update software regularly
3. Implement MFA
4. Train employees in security awareness
5. Deploy NAC solutions
6. Encrypt sensitive data
7. Secure Wi-Fi networks
8. Conduct regular security audits and assessments
9. Establish access management policies
10. Develop an incident response plan

Figure 8 : Unauthorized Access: How to Prevent It & Protect Your Data

V. SIGNIFICANT VULNERABILITIES IN MARITIME CYBERSECURITY

The maritime industry, which plays a pivotal role in the world trade and transport sector, is at higher risk from cyber threats as it has shifted towards computerization. These elements worsen these vulnerabilities: infrastructure and information technology are old, poor protection of networks and systems, the connection of IoT devices, and the difficulties of third-tier suppliers. This section, reviewing the principal threats in the maritime domain, presents the main threats in maritime cybersecurity.

1. Aging Infrastructures and Outdated IT Systems

It has been established, for instance, that one of the significant risks is that most of the ships and ports in the contemporary world still employ architectures that have yet to be developed with newly emerging cybersecurity threats in mind. Older systems need to have essential updates which can help improve security and prevent cyber incidents (Wei et al, 2010). However, upgrading such systems becomes very expensive and sometimes practically impossible because these establishments must run 24/7, especially in ports or on ships at sea. Integration of this newer technology with these older systems also brings compatibility problems and, consequently, a downturn in security. For example, an old system may not support such features as encryption or different factor identifiers to prevent access. This was well demonstrated when Maersk was attacked in 2017 by ransomware, which paralyzed the company partly because of outdated systems.

2. Poor Cybersecurity Protocols and Lack of Awareness Among Staff

The ten main human factors contributing to cybersecurity risks in the maritime industry include the following: These risks are increased by weak protection from cyber-attacks due to a need for more awareness among the staff. Inexperienced employees who have yet to receive specific training in cybersecurity threats can become threats themselves by accidentally compromising key processes due to their mistakes; for example, they can click on a phishing link or use unsafe passwords. Measures of training and awareness need to go further, and many crews and port employees need to prepare for the actual cyber threats they encounter. Phishing and spear-phishing are the most frequent social engineering types this sector embraces. They capitalize on the Trusted relations that people have for their colleagues or relatives and also the negligence of people. Thus, the first action to enhance endpoint security is to strengthen the general IT security policies and make the staff members more knowledgeable of possible risks.

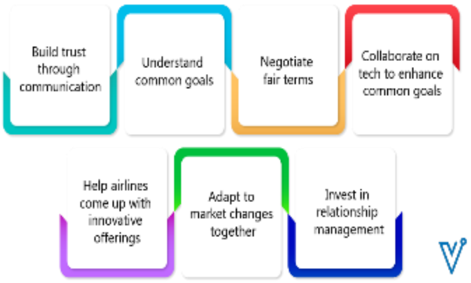

Build trust through communication
Understand common goals
Negotiate fair terms
Collaborate on tech to enhance common goals
Help airlines come up with innovative offerings
Adapt to market changes together
Invest in relationship management

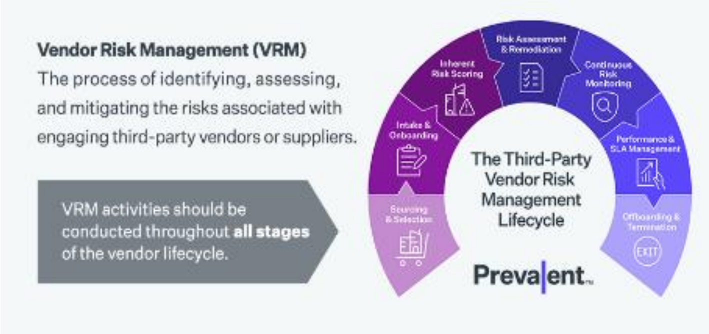
Figure 9: Navigating Airline Relationships as an OTA: Tips for Success

3. Integration of IoT Devices and Increased Network Complexity

IoT devices in the maritime industry have also intensified, adding pressure on the cybersecurity department. Today, cruise ships and ports contain many connected devices that sense and interact with their environment, from simple sensors and control systems to entertainment devices. These devices increase operation efficiency, provide a better customer experience, and bring vulnerability. The connectivity gargets of IoT are typically less potent in processing and memory, which means that high-end measures such as encryption and firewalls are hard to implement (Maheshwari & Dagale, 2018). For this reason, these devices can turn into unguarded doors through which cybercriminals can access the more extensive network. Moreover, the new level of maritime networks' interaction, established between multiple interconnected devices, increases the threat level. Because the car's systems are interconnected in many cases, a problem in one area could quickly manifest in others, including navigation systems, engine controls, and cargo handling. One of the most recent GPS spoofing was in the Black Sea earlier this year, where vessels were misled about their positions; this shows how IoT systems are at risk.

4. Challenges of Managing Third-Party Vendor Relationships

The other major problem arising from the dependence of this sector on third parties for significant services such as port operations, logistics, and other onboard technologies is the need for more protection against cyber-attacks found in maritime cybersecurity. Most of these merchants are vendors and work closely with sensitive networks within the maritime network; a single-point compromise will lead to a domino effect on the rest of the systems. Government procurement of goods and services includes having third-party vendors provide and maintain those goods and services; managing and ensuring the cybersecurity of those third-party vendors is a daunting task (Vitunskaite et al, 2019). The vendors with which the leading organizations collaborate are likely to have diverse and weaker security measures than the primary business entities. For instance, a vendor working with a ship vendor could inadvertently bring malware into a ship's operating system through an untested update. These supply chain attacks have grown rampant as long as the hackers know they can leverage vulnerable aspects of those vendors' systems to penetrate usually more secure organizations. For these risks to be managed effectively, a vendor must comply with and adhere to standard cybersecurity, and the vendor's practice should be audited frequently.



Vendor Risk Management (VRM)

The process of identifying, assessing, and mitigating the risks associated with engaging third-party vendors or suppliers.

VRM activities should be conducted throughout **all stages** of the vendor lifecycle.

Risk Assessment & Remediation
Inherent Risk Scoring
Continuous Risk Monitoring
Intake & Onboarding
Performance & SLA Management
The Third-Party Vendor Risk Management Lifecycle
Sourcing & Selection
Offboarding & Termination
EXIT
Prevalent

Figure 10: Vendor Risk Management: 8 Keys to Success

VI. DATA PRIVACY AND PASSENGER INFORMATION

Gathered passenger data of cruise ships can include many facts to improve service quality, security, and organization. However, this search for information intensiveness leads to severe violations of this fundamental human right. There is little doubt that significant advances are taking place in using digital technologies and internet connectivity on ships (Till, 2013). While this brings safety, convenience, and efficiency benefits, passenger data can also be at risk from breaches. This section looks at the various aspects of passenger information collected, the vulnerability inherent in the custody of personal information, the universal measures regarding privacy, and how the shipping industry meets these standards.

1. The type of passenger Information processed on cruise ships

Cruise lines collect the following types of passenger data during booking, embarkation, and cruise voyages. Such data enhances company service, guarantees customer protection, and meets legal obligations. Common categories of passenger data include:

A. Payment Details: Cruise ships collect large quantities of consumers' credit card details and bank account numbers. This data is used to book services, make onboard purchases, and organize excursions. Any invasion of this information may result in identity theft and financial fraud, thus the need for cruise lines to guard payment information.

B. Health Information: Because the safety of passengers is of paramount importance, cruise lines take a history of medical conditions, including allergies and current and previous medical conditions, and contact information collection histories are instrumental in data and mining the proper treatment that should be offered during the voyage. However, health information about the collection also falls under the proper treatment to offer during wrong hands.

C. Travel Preferences and Behaviours: Fall lines watch their partners via Pa's purchase pattern if it falls into eating habits, interests, and other related purchases. It also enables cruise companies to build better experiences that enhance customer satisfaction. Nonetheless, identity theft or other malicious use or leakage of this information will likely be abused, profiled, or exploited by hackers and other malicious actors.

D. Location and Surveillance Information: Cruise ships today have a man who will likely be abused, e.g., using key cards, wristbands, or any technology for security and practical cruise functionality. Surveillance systems and other access controls also collect data, which is essential for security on board (Lyon, 2014). Any violation of location information means that passengers are vulnerable to physical danger or stalking.

2. Risks of Data Breaches in the Maritime Industry

The maritime industry has become highly susceptible to data breach attacks because it depends on integrated systems and carries profound data-gathering activities. A data breach is a situation whereby unauthorized parties gain unauthorized access to sensitive information due to hacking illicit activities or due to insiders (Kolevski et al, 2021). In the cruise industry, information technology breaches are very dangerous because they can lead to loss-making, compromise the company's image, and attract litigation. One of the significant difficulties is that maritime systems encompass on-board media and communication systems and operational technologies. This opens up the networks to possible cyber-attacks. For example, low encryption standards or missing updates can lead to the hacking of passenger data, resulting in identity or financial fraud. Thirdly, using third parties in the complex and integrated maritime supply chain poses a high risk of a breach. Outsourced service providers such as SATCOM and payment systems can pose risks if the suppliers are not exceptionally cautious with cyber security. An intrusion in a third-party system could compromise the whole network of the cruise line company and cause many data losses.

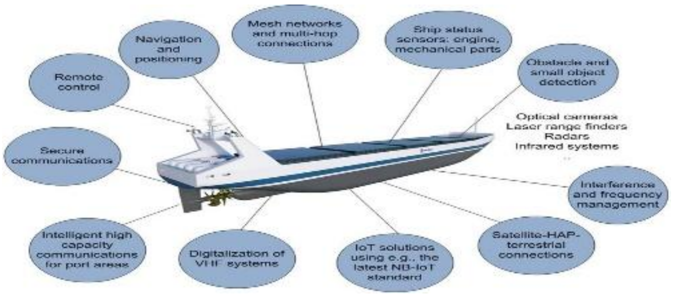

Navigation and positioning
Mesh networks and multi-hop connections
Ship status sensors: engine, mechanical parts
Remote control
Obstacle and small object detection
Optical cameras
Laser range finders
Radars
Infrared systems
Secure communications
Interference and frequency management
Intelligent high capacity communications for port areas
Digitalization of VHF systems
IoT solutions using e.g., the latest NB-IoT standard
Satellite-HAP-terrestrial connections

Figure 11 : Connectivity challenges of an autonomous ship

3. Compliance with Global Privacy Regulations

In becoming an acceptable solution to the challenges posed by data breaches, the cruise lines are subject to multiple global privacy regulations. These regulations guide how passengers' data should be captured, managed, and secured so that each cruise operator deploys the best practices in data protection.

A. General Data Protection Regulation (GDPR): The GDPR relates to passengers from the EU only and requires organizations to be transparent about collecting data. Risk to Customers: Cruise lines are legally obligated to treat passengers on the PII they collect – the kind, amount, frequency, and purpose; they are required to provide guests with unequivocal notice of this above information (Perritt, 1996). Again, passengers have the right to obtain or request for the erasure of such data to retain sovereignty over their data.

B. Payment Card Industry Data Security Standard (PCI DSS): Any organization dealing with payment card data is bound to adhere to the PCI DSS standards, which set a strict standard for payment card transactions. This is accomplished by eliminating the transfer of payment details in the clear and restricting access to secure financial data to personnel from the financial section ONLY.

C. Health Insurance Portability and Accountability Act (HIPAA): HIPAA regulates the use of health information in the USA, especially with cruise lines that offer medical facilities on their ships. Adherence to HIPAA assures that passengers' medical records regarding their medical conditions are safe from disclosure and only retrievable by authorized medical practitioners.

4. Best Practices for Protecting Passenger Data on Ships

To minimize data breach risks, cruise lines several can employ best practices.

A. Data encryption must be applied to all databases, and information must be transmitted between the server and clients or stored in the server (Hacigumus et al, 2002). This also allows us to keep innovating how we handle data so that even if the data is intercepted, the adversary cannot decipher it, let alone leverage it to their advantage.
B. Cruise operators must implement complex passwords through Multi-Factor Authentication (MFA). MFA provides a higher level of security because it insists on using two or more factors before one can access data. This method helps reduce the danger of using collapsed or stolen passwords.
C. Network segmentation will prevent extensive losses should there be an attack. By separating some of these operational systems from the networks accessible to passengers onboard, cruise lines may mitigate the chance of an attacker obtaining credentials through infected entertainment or Wi-Fi systems.
D. Constant cybersecurity training should be provided for seamen and passengers carrying gadgets. Staff should be informed on identifying phishing scams and other cyber events, and passengers should be informed about protecting their information whenever they use internet services on airplanes (Lin & Goodman, 2007).

VII. CYBERSECURITY BEST PRACTICES FOR THE MARITIME INDUSTRY

Cyber security problems, part of the maritime industry, are becoming increasingly urgent in the current world economy. Advanced digital technologies during shipping operations create entry points, and cyber security problems are increasingly exploited to compromise the integrity of vessels and breach supply chains, which is always bad for businesses. Therefore, for an organization to embrace strong cybersecurity practices is mandatory. The following general cybersecurity measures have been recommended considering the specific cyber threats in the maritime industry: Network segmentation, Establishing patching and update regimen, use of encryption, Multi-factor authentication, Physical security, Continuous monitoring, and Incident response plan.

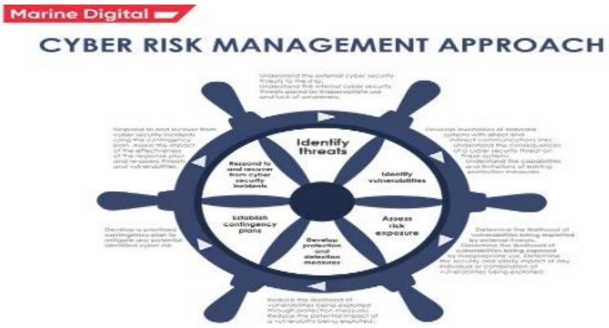

Marine Digital
CYBER RISK MANAGEMENT APPROACH
Identify threats
Identify vulnerabilities
Assess risk exposure
Develop protection and detection measures
Establish contingency plans
Respond to and recover from cyber security incidents

Figure 12: The importance of cybersecurity in the maritime industry

1. Network Segmentation

Network segmentation is one of the best cybersecurity practices that should be practiced within maritime business operations. There are two main strategies, which are network segmentation and data segmentation. Network segmentation means that various network components are isolated to restrict access to essential system sections (Cruz, 1991). Some of the measures include Network segmentation, which involves separating operational technology (OT) systems, such as those that control the navigation engine management and cargo handling, from the everyday, general IT, or the guests' network, thereby minimizing the exposure of such OT system operations to outside interference. Separating these guest networks from the systems indispensable for hotel functioning helps exclude the adversary's possibility of navigating the network area in case he or she gets into the network via a more vulnerable gateway. For instance, passengers' or crew' devices should have limited connectivity to other networks accessing the non-essential parts of an MPS ship's network. Second, the differentiation of the networks makes it simpler to supervise the increased number of segments and respond to security incidents instantly.

2. Regular Patching and Systems Updates

This environment is as volatile as the maritime industry itself. Thus, the Software and the hardware in use require frequent upgrades to protect against such threats. This is bad because systems with unapplied patches allow malware, ransomware, and other malicious programs to enter the network since the old version usually contains unaddressed risks. Updating the shipboard systems and their Software often reduces vulnerability since it opens the system to standard security features. Due to the nature of the ship's operation, there is a need to develop a schedule for patches and updates, no matter how the ship in question may be. Software vendors usually develop antidotes to new threats by creating patches; hence, following these patches as a best practice in information security is essential.

3. Encryption and Secure Communication

Keeping information and data, such as the specifics of the cargo being transported, geographical position, and details of passengers on board a vessel, are significant challenges for maritime cybersecurity. Encryption can be more of a safeguard since it authenticates data and puts it in a form other parties cannot understand during transfer and storage (Wang et al, 2010). Complete end-to-end encryption means that only the intended recipient has the authority to access the message's contents, and hackers cannot con him or her. Functionalities applied in the maritime industry and those encompassing operation control and data transmission should observe high levels of encryption. For example, encrypted satellite communications, which can be used for monitoring distant vessels, or VoIP systems, which can be used for secure verbal communication, considerably enhance a ship's protection against violation and data theft.

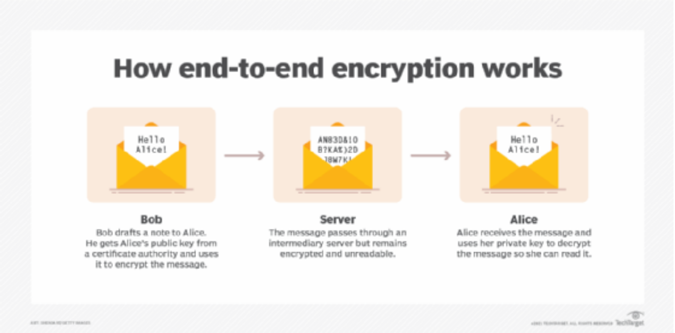

How end-to-end encryption works
Hello Alice!
AN83D&10 B?KA£)2D J8W7K!
Hello Alice!
Bob
Bob drafts a note to Alice. He gets Alice's public key from a certificate authority and uses it to encrypt the message.
Server
The message passes through an intermediary server but remains encrypted and unreadable.
Alice
Alice receives the message and uses her private key to decrypt the message so she can read it.
TechTarget

Figure 13: What is End-to-End Encryption (E2EE) and How Does it Work?

4. Multi-Factor Authentication (MFA)

The second proven access control mechanism is multi-factor access control, which is known to strengthen the protection of critical systems. MFA insists that users provide two or more identification factors, for instance, a password and a code issued to a personal device. This layered means of improving security guarantees that even if a hacker gets one type of access credentials, he cannot access the system without a second and third factor of security authentication, making it very hard for a malicious person to breach the security system. In context with marine operations, MFA can be implemented to limit the interaction with areas of the ship, including the control system, administrative access, and other forms of remote controlling and access, hence augmenting the security of the entire ship network.

5. Physical Security of IT Systems

These threats mainly express themselves as cybersecurity attacks, but physical access control still plays an equally important role, especially when approaching crucial IT systems onboard ships. Security measures such as limiting access to control rooms, data servers, and other computer hardware prevent cases where physical access to prepare modifications is allowed, or IT equipment is utilized without proper permission. Physical assets used by the maritime industry should be protected with security measures, such as access control, surveillance, and the setting of restricted physical security zones (Helmick, 2008). For example, control rooms should have key card accesses; CCTV should be installed to monitor restricted areas because such areas will go a long way in minimizing the instances of a breach and, to top it all up, record the breach if such a situation arises.

6. Continuous Monitoring and Threat Protection

The difference between continuous monitoring and threat detection is that continuous monitoring requires constant vigilance in looking for threats in a system and checking for compliance during regular system monitoring. An effective identification of suspicious activities in the network requires constant surveillance of network activities. This is a relatively new concept in technological risk management, where maritime organizations use various tools, including IDS, IPS, and advanced analytics, to monitor their network for malicious activities before such activities occur. Intrusion detection systems define baseline traffic patterns and security IOCs that show signs that a cyber-attack may be occurring. Continuous monitoring also enables quick action since security personnel are informed immediately to take corrective measures and prevent much damage.

7. Incident Response and Recovery Plans

Maritime cybersecurity is a growing concern, and the reality is that anyone operating in the industry needs to be ready for a potent incident response and recovery scenario. Some cyberattacks can be unexpected, and creating a contingency plan helps maritime organizations to avert longer downtimes when under attack. Incident response management should state how to contain the systems involved, determine the degree of effect, and engage other actors to bring order. Also, routine testing and practicing of these plans create awareness of the course of action to be taken in case of the actual occurrence of the incident, as it helps reduce confusion (Donahue & Tuohy, 2006). Contingency measures also require assessment after the incident to determine the loopholes that need to be closed in order to improve the future strength of cybersecurity measures.

VIII. CHALLENGES IN IMPLEMENTING CYBERSECURITY MEASURES IN THE MARITIME INDUSTRY

The maritime industry, a significant global economy driver, is threatened by hackers and other malicious actors as the use of advanced technologies grows. However, cybersecurity measures face diverse barriers to implementation in this industry: geopolitical factors, compliance barriers, crew shortage effects, and budget constraints. It is essential to overcome these challenges to save maritime operations, but complexity often intervenes in the efficient decision-making of cybersecurity plans.

1. Geopolitical risks and compliance challenges

Maritime is a world industry where transactions occur across international borders, and sometimes, there are different cybersecurity norms and laws. This diversity poses a compliance challenge since the shipping companies are forced to work under the laws of each country. This makes it more challenging to be consistent with cybersecurity regulations. Forgery of the security standards of different countries may cause some security gaps. For example, a vessel meeting the cybersecurity regulation of one country may not meet another's regulation, which means that the vessel can be venerably exposed to cyber threats in some countries with less rigorous policies. The escalation of tensions of a geopolitical nature continues to compound cybersecurity threats in the maritime business. In an industry where many vessels navigate politically charged waters, this threat from state-backed actors is all the more real. For example, during geopolitical rivalry, unfriendly forces can attack shipping channels to pressure or deny the opposing side the opportunity to conduct their business. More caution must be embraced in such regions because cyber threats may be complex and politically inclined and attack navigational systems, port activities, or supply chain information. Therefore, the shipping industry is pressured to dedicate resources to effective security enhancement. This can be problematic due to the disparity of regulation in this domain and the regional disparity of threats.

That is why the IMO tried to solve these problems and initiated the International Safety Management (ISM) Code, including cybersecurity management. However, regulatory enforcement differs significantly, and organizations need help adhering to standard cybersecurity measures and norms. An even more significant problem is that most SMEs in the maritime sector need more funds and knowledge to attain full conformity, all of which makes the industry's cyber defense even more fragile. Consequently, cooperation and unification of rules promote the strengthening of global cybersecurity and minimize the negative influence of geopolitical factors on maritime cybersecurity.

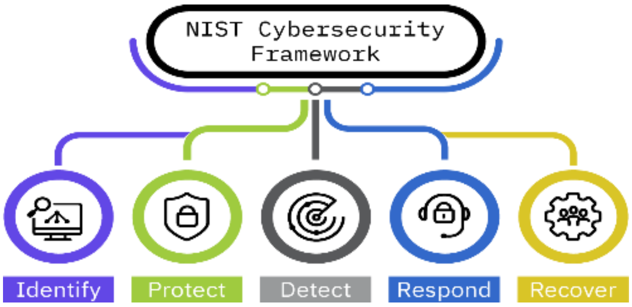


Figure 14: Three Steps to Ensure IMO/ISM Cybersecurity Compliance

2. Impact of Crew Shortages on Operational Safety and Cybersecurity

There have always been challenges related to crew availability in the maritime business, and the impact has reached safety and cyber risk areas. Every day, senior and experienced seafarers resign or retire, and since there is little training on cybersecurity, the vessels are left open to cyber threats. Contemporary vessels have an extensive dependence on digital systems and components, and an ineffective crew may place the ship's digital systems in harm's way either by accident or by mishandling assets. New employees and contractors may need to become more familiar with what can occur from a cybersecurity threat, such as the fall for a phishing scheme, malware, or a data breach. Additionally, crew deficiency can increase the remaining personnel's burden, which can cause fatigue and weak compliance with cybersecurity measures (Gasser, 1988). The crew member becomes tiresome and can hence ignore set security measures or neglect to identify any abnormality taking place in the vicinity. As the ships are always at sea and manned by round-the-clock crews, the employees can easily neglect conventional cybersecurity tasks like updating Software, scanning for vulnerabilities, and monitoring the network's traffic. This risk is fueled by the need for more emphasis on cybersecurity in conventional programs in maritime learning institutions, hence the need to develop specialized security courses for the maritime industry.

New intelligent applications and technologies have been suggested to help reduce the effect of crew scarcity on cybersecurity. However, these technologies are capital-intensive; implementing them also opens up other risks that must be addressed. Maritime organizations need to find a way to relieve workforce pressure and, at the same time, avoid exposing automation technologies to hackers. As the crew deficits continue, the need to recruit cybersecurity littermates and automate the protection of its digital networks becomes dire for the maritime business.

3. Financial Constraints in Adopting New Technologies

Another considerable challenge is a need for more funds, which results in cybersecurity in the context of the maritime industry staying weak. Ultimately, integrating advanced cybersecurity solutions may be expensive, and many SME rivals in the maritime industry may need to be able to afford costly measures. Several sources of financial pressure limit the effectiveness of the technology adoption. These restrictions lead to ancient technology integration and heavy reliance on outdated systems that can easily be hacked. However, deploying cybersecurity infrastructures entails recurrent costs as maintenance, updates, and staff training are compulsory to sustain a strong shield against cyber threats. To partly or wholly compensate for this, companies must generate more cash, which places continuous pressure on financial resources – a nut of residuals in any field with narrow profit margins. Whereas resident giants of the shipping industry must certainly afford sophisticated cybersecurity measures, resources are often scarce for SMEs, making for appealing targets for cybercriminals (Chaitoo, 2000). The industry is also limited by financial factors in applying new technologies like AI and block chain and better security, such as advanced encryption, which could further improve the industry's security but require more capital investment. This reality increases risk as numerous maritime organizations lacked sufficient funding to protect all aspects of their operations despite the availability of countermeasures.

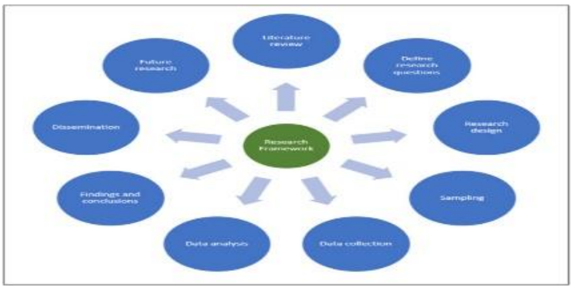


Figure 15: Perspective of small and medium enterprise (SME's)

Cybersecurity, nevertheless, costs businesses much more than the price needed to secure them against the growing threats on the internet. The consequences of successful cyber attacks are hindered business operations, more excellent financial organizing, the tarnished image of an organization, and fines from regulating authorities. Therefore, maritime companies are trapped between catering to current financial loss control and securing funds for protective cybersecurity measures to prevent more considerable, devastating losses. The attempts to support financial investments or offer specific cybersecurity incentives for the companies and organizations operating within the maritime domain can contribute to the challenges and improvement of the general industry.

IX. REGULATORY COMPLIANCE AND INTERNATIONAL STANDARDS

Due to rapid enhancement in IT and Communication, it has become more important that proper legal authority intervention occurs in telematics, asset tracking, and personal data Communication industries. The following focuses on critical international regulations: the IMO cybersecurity recommendations, the GDPR, and the PCI DSS regulation (Mthembu, 2019). These regulations are vital in protecting passengers' data and the general operation safety of the companies. However, the challenge of following multiple international standards is twofold, as companies try to overcome multiple legal barriers across different countries. This discussion highlights the role of regulation in promoting assertiveness, data security, and enhanced operational efficiency.

1. Key Regulations Overview

- The ITU has three recommendations concerning cybersecurity that have been established in IMO: The IMO developed cybersecurity recommendations to strengthen the existing framework for the swift running of the maritime sector. The IMO guidelines, known as the Maritime Security (MARSEC) level 3, which was published under Resolution MSC.428(98), have an objective of reducing cyber risks in the global shipping business by including the safety measures in the shipping companies' Safety Management Systems (SMS) by next year. These recommendations address the use of digital systems in shipping, which has grown, and exposure to cyber threats threatens ship safety and business continuity. The IMO recommendations cover inherent risk appraisal, protective steps, and incident handling methodologies to enhance companies' approaches to cybersecurity risks.
- General Data Protection Regulation (GDPR): The GDPR regulates the use of personal data in the EU and the European Economic Area and was put into force in 2018. It seeks to protect the PII and the privacy of EU citizens with a focus on, among other things, information disclosure,

data processing limitation, and responsibility. The regulation applies to organizations within and outside the EU that control or process the data of EU citizens,' data, making it relevant to international businesses that engage in telematics, asset tracking, and or fleet management. Failure to adhere to the GDPR rules leads to heavy punishments, fines of €20 million or 4% of the firm's total worldwide turnover. The GDPR requires people in charge of organizations to have prior permission from people before collecting or using personal details, applying protection measures for the data, and informing of breaches within three days.

- Payment Card Industry Data Security Standard (PCI DSS): PCI DSS is an international information security standard implemented to protect cardholder payments by safely handling, processing, storing, and transmitting card information. PCI DSS compliance becomes a requirement for organizations that accept credit card information, and this involves organizations that deal with telematics for payment or fleet servicing. The standards mandate access control provisions, cardholder data encryption, continued card and system monitoring, and system vulnerability assessment. With the implementation of PCI DSS, the risk of fraud is significantly minimized, especially for organizations that accept payments through telecommunication systems.

2. Challenges in Complying with Multiple International Regulations

Implementing IMO cybersecurity recommendations, GDPR, and PCI DSS has problems for telematics, asset tracking, and fleet management companies. They are primarily international industries because they involve the sale of goods and services across countries' borders with different laws on the same subject. For example, GDPR is designed to protect the citizens' data of the EU member states and PCI DSS – to ensure the security of payment cards. At the same time, IMO recommendations require cybersecurity to be essential to the maritime industry. Coordinating these many and diverse regulations can be a logistical nightmare, especially for organizations that may not possess significant resources or specialized knowledge in the regulatory environment. Another problem is that the rules and regulations evolve continuously. The emergence of new threats and issues with data security leads to changes in regulations that may need to be coordinated and may change from region to region or industry to industry. The constantly changing regulatory environment for organizations also implies constantly reviewing and seeking to improve compliance programs, which is time-consuming and costly (Hunt & Auster, 1990). For instance, GDPR imposes very high data protection requirements that require sound data handling and storage measures, which may interfere with or complement those required for PCI DSS compliance. However, these requirements are cross-functional, and specific issues may arise. Each functional department or unit may have its concerns and regulations. Its requirements may be bravery, but it also creates barbed wire consolidation within the functioning organization.

3. Importance of Following Regulations to Protect Passenger Data and Maintain Operational Safety

Regulation of compliant architecture is essential to ensure the confidentiality of information and physical safety for operations. Adherence to rules like GDPR improves the protection of the customers' information, encouraging a positive attitude toward the organization's management of personal data. This is particularly true in telematics and fleet management applications, where location and personal data are collected and transmitted in real-time. In this sense, regulatory compliance minimizes the danger of other people accessing the information and possible misuse, thus protecting customers' information and the organization's reputation. As with IMO cybersecurity recommendations, IMO cybersecurity suggestions are equally essential to guarantee the safety of the operations in the maritime business. Since vessel systems are very much integrated, there is a high probability that cyber risk will affect navigational and operation features (Fan et al, 2020). With IMO's recommendations on cybersecurity in place, more risks for cyber threats that may affect ships' control systems, resulting in accidents or operational disturbances, can be averted. Adherence to IMO guidance ensures that ship operators have developed cyber risk mitigation procedures and implemented response procedures in cases of such occurrences, which is very important in preventing the effects of cyber incidents on the operations of the vessels.

It is important to note that PCI DSS has to be implemented in the same way to protect payment data and reduce risk for companies in connection with the consequences of data breaches. At telematics firms that deal with the processing of payments, implementation of the PCI DSS assists in defending the customer's payment card information from fraudsters, hence limiting fraud cases. Therefore, failure in PCI DSS compliance puts organizations at risk of fines and makes them prone to financial fraud losses. Hence, the assessment and compliance with the PCI DSS are a method of gaining customer trust in payment security and upholding the financial solvency of the telematics business.

X. CONCLUSION

As the world becomes more connected, reliable cyber defence becomes paramount to protecting the maritime industry from even higher cyber-attacks. The maritime industry, being a global trade and supply chain essential, centers on interdependent embedded systems, ranging from navigation gadgets and instruments, communication systems, monitoring and tracking of cargo, and other assets. Given that attacks against this critical infrastructure have increased significantly, it means that now, more than ever, a sound cybersecurity shield is required. The integration of sophisticated cybersecurity models and standards into the management of marine activities safeguards resources. It maintains functions during adversities, consequently strengthening the non-invasion of cybercrime in the maritime sector. Nyati (2018) identifies ways existing asset tracking and efficiency innovations can be extended to the maritime field to help mitigate these risks and improve security across the industry.

Specifically, the perpetual advancement of various technologies that work within the maritime industry, the new regulations, and the awareness of cyber threats are the main factors for future cyber security developments in the maritime industry. The improvements in telematics, real-time monitoring, and algorithms will shift how maritime operations approach cybersecurity. For instance, advanced telematics is capable of real-time asset tracking that increases awareness of threats such as cyber intrusion and other unlawful entry into the asset. Besides, advances in dispatching and algorithms for the fleet can effectively fit into maritime logistics operations without exposing it to cyber risks. They are enablers of organizational efficiency and invaluable sources for the detection, risk management, and handling of cyber security threats. The advancement in cyber security in the maritime context will likely prevent tools like predictive analytics, artificial intelligence, and machine learning from effective threat identification and management in real time.

It remains imperative for the players in the maritime industry to come up with shared solutions to guarantee a safe future. Governments, shipping firms, and cybersecurity professionals must collectively formulate secure practices that meet the segment's demands. Authorities can be considered critical drivers for determining norms and standards that have to be complied with by organizations and companies in international waters. They can also enable information sharing, for instance, helping companies exchange critical intelligence relating to new threats and weaknesses in cyberspace at the right time. On its part, shipping companies must rise to the challenge of establishing well-boned cyber security and making employees understand the importance of cyber security in their companies. Information security specialists have technical know-how, which empowers them to help companies address distinct types of cyber risks and design approaches to organizational tasks. Such defence collaborations enhance the synchronization and the overall strength of maritime cybersecurity since players all work towards the same common goal. Maritime security relies on close collaboration among private and public companies because a stable and comprehensive response to cyber threats can only be developed through teamwork and the qualified opinion of cybersecurity experts. Consequently, the maritime industry's journey to achieve a state of cybersecurity readiness best described as 'resilience' is long and complex but has to be done. For this reason, this article provides insights into how integrating IT technologies, regulatory compliance, and stakeholders' cooperation can reduce cyber threats to international supply chains. Realizing a safe environment in naval activities is not simply a win-win situation but a guaranteed way to protect the field's present and future and the world's economic and business systems.

REFERENCES

1. Andreadakis, A., & Sloane, T. (2021). An automated lifeboat, manifesting embarkation system (ALMES): the utilization of RFID/NFC in passenger manifestation during ship evacuation.
2. Berle, Ø., Asbjørnslett, B. E., & Rice, J. B. (2011). Formal vulnerability assessment of a maritime transportation system. Reliability Engineering & System Safety, 96(6), 696-705.
3. Burrell, J. (2012). Producing the Internet and Development: an ethnography of Internet cafe use in Accra, Ghana (Doctoral dissertation, London School of Economics and Political Science).
4. Chaitoo, R. (2000). Electronic Commerce and CARICOM Economies.
5. Cruz, R. L. (1991). A calculus for network delay. I. Network elements in isolation. IEEE Transactions on information theory, 37(1), 114-131.
6. Donahue, A., & Tuohy, R. (2006). Lessons we don't learn: A study of the lessons of disasters, why we repeat them, and how we can learn them. Homeland Security Affairs, 2(2).
7. Fan, C., Wróbel, K., Montewka, J., Gil, M., Wan, C., & Zhang, D. (2020). A framework to identify factors influencing navigational risk for Maritime Autonomous Surface Ships. Ocean Engineering, 202, 107188.
8. Gasser, M. (1988). Building a secure computer system (p. 85). New York: Van Nostrand Reinhold Company.
9. Gill, A. (2018). Developing A Real-Time Electronic Funds Transfer System for Credit Unions. International Journal of Advanced Research in Engineering and Technology (IJARET), 9(1), 162-184. https://iaeme.com/Home/issue/IJARET?Volume=9&Issue=1
10. Hacigumus, H., Iyer, B., & Mehrotra, S. (2002, February). Providing database as a service. In Proceedings 18th International Conference on Data Engineering (pp. 29-38). IEEE.
11. Hayes, C. R. (2016). Maritime cybersecurity: the future of national security (Doctoral

dissertation, Monterey, California: Naval Postgraduate School).

12. Helmick, J. S. (2008). Port and maritime security: A research perspective. Journal of Transportation Security, 1, 15-28.
13. Hunt, C. B., & Auster, E. R. (1990). Proactive environmental management: avoiding the toxic trap. MIT Sloan Management Review, 31(2), 7.
14. Kolevski, D., Michael, K., Abbas, R., & Freeman, M. (2021, July). Cloud data breach disclosures: The consumer and their personally identifiable information (PII)?. In 2021 IEEE Conference on norbert wiener in the 21st century (21CW) (pp. 1-9). IEEE.
15. Lin, H. S., & Goodman, S. E. (Eds.). (2007). Toward a safer and more secure cyberspace. National Academies Press.
16. Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. Big data & society, 1(2), 2053951714541861.
17. Maheshwari, N., & Dagale, H. (2018, January). Secure communication and firewall architecture for IoT applications. In 2018 10th International Conference on Communication Systems & Networks (COMSNETS) (pp. 328-335). IEEE.
18. Mehan, J. (2016). Insider threat: A guide to understanding, detecting, and defending against the enemy from within. IT Governance Ltd.
19. Mitnick, K. D., & Simon, W. L. (2009). The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers. John Wiley & Sons.
20. Mthembu, S. N. (2019). Navigating the complex maritime cyber regime: a review of the international and domestic regulatory framework on maritime cyber security (Doctoral dissertation).
21. Nyati, S. (2018). Revolutionizing LTL Carrier Operations: A Comprehensive Analysis of an Algorithm-Driven Pickup and Delivery Dispatching Solution. International Journal of Science and Research (IJSR), 7(2), 1659-1666. https://www.ijsr.net/getabstract.php?paperid=SR24203183637
22. Nyati, S. (2018). Transforming Telematics in Fleet Management: Innovations in Asset Tracking, Efficiency, and Communication. International Journal of Science and Research (IJSR), 7(10), 1804-1810. https://www.ijsr.net/getabstract.php?paperid=SR24203184230
23. Perritt Jr, H. H. (1996). Jurisdiction in cyberspace. Vill. L. Rev., 41, 1.
24. Ryan, M. (2020). The ransomware revolution: how emerging encryption technologies created a prodigious cyber threat (Doctoral dissertation, UNSW Sydney).
25. Till, G. (2013). Seapower: A guide for the twenty-first century. Routledge.
26. Venizelou, C. (2018). Operational crisis management and the influence of cyber-Threats and external fraud to business continuity planning in international banking industry.
27. Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. Computers & Security, 83, 313-331.
28. Wang, C., Wang, Q., Ren, K., & Lou, W. (2010, March). Privacy-preserving public auditing for data storage security in cloud computing. In 2010 proceedings ieee infocom (pp. 1-9). Ieee.
29. Wei, D., Lu, Y., Jafari, M., Skare, P., & Rohde, K. (2010, January). An integrated security system of protecting smart grid against cyber attacks. In 2010 Innovative Smart Grid Technologies (ISGT) (pp. 1-7). IEEE.