UNIVERSITY OF PIRAEUS

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
DEPARTMENT OF DIGITAL SYSTEMS

MASTER'S THESIS

Navigating the Waters of Maritime Cybersecurity with BIMCO's Guidelines: Identifying Vulnerabilities and Mitigating Threats to IT and OT Systems

Georgios Kalogeras

Supervisor:
Christos Xenakis, Professor

PIRAEUS

OCTOBER 2023

MASTER'S THESIS

Navigating the Waters of Maritime Cybersecurity with BIMCO's Guidelines: Identifying Vulnerabilities and Mitigating Threats to IT and OT Systems

Georgios Kalogeras

A.M.: MTE2107

ABSTRACT

This master's thesis examines vulnerabilities and related protection methods for OT and IT systems in vessels used in the marine sector, incorporating guidelines and methodologies from BIMCO in the review process. This study comprises a review of possible cybersecurity threats to these systems, mitigation strategies for those risks, and an examination of the IT and OT systems on board a ship. The study's findings show that the marine sector is vulnerable to various cybersecurity threats and that efficient protective measures must be implemented to mitigate these risks. The unique vulnerabilities and security controls that should be considered for IT and OT systems in vessels are discussed in this thesis.

SUBJECT AREA: Cybersecurity in the maritime industry with BIMCO’s guidelines. Vulnerabilities and protection measures for IT and OT systems in vessels.

KEYWORDS: Cybersecurity, Maritime, BIMCO, Vulnerabilities, Protection Measures, Risk Mitigation

ACKNOWLEDGMENTS

First and foremost, I would like to express my sincere gratitude to my supervisor, Professor Christos Xenakis, for his guidance, support, and encouragement throughout my master's thesis. His insightful feedback and suggestions have been invaluable.

I would also like to thank my advisor and Ph.D. candidate in our department, Aristeidis Farao, for his assistance and mentorship in completing this thesis. His expertise and guidance have been instrumental in shaping the methodology and approach of my research.

Finally, I would like to thank my family and friends for their unwavering support and encouragement throughout my academic journey. Their understanding and encouragement have been a constant source of motivation and inspiration.

This Page Intentionally Left Blank

List of Figures

List of Tables

List of Abbreviations

AIS	Automatic Identification System
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
ARPA	Automatic Radar Plotting Aids
BIMCO	Baltic and International Maritime Council
BYOD	Bring Your Own Device
CCTV	Closed Circuit Television
CIRM	Comité International Radio-Maritime
CSIRT	Cyber Security Incident Response Teams
CTI	Cyber Threat Intelligence
CISO	Chief Information Security Officer
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoC	Document of Compliance
ECDIS	Electronic Chart Display and Information Systems
EDR	Endpoint Detection and Response
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HMI	Human Machine Interface
HSM	Hardware Security Module
ICT	Information and Communication Technology
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IMO	International Maritime Organization
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISM	International Safety Management
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LR	Lloyd's Register
MAC	Media Access Control
MFA	Multi-Factor Authentication
MTTR	Mean Time to Repair
NAC	Network Access Control
OFE	Optimistic Fair Exchange
OS	Operating System
OT	Operational Technology
PIN	Personal Identification Number
RAT	Remote Access Trojan
SDN	Software Defined Network
SIEM	Security Information and Event Management
SOC	Security Operations Center
SSP	Ship Security Plan
TOTP	Time-based One Time Passcode
TPM	Trusted Platform Module

USB	Universal Serial Bus
VDR	Voyage Data Recorder
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network

TABLE OF CONTENTS

1. Introduction

The maritime sector now faces both new capabilities and risks as a result of its growing reliance on information technology (IT) and operational technology (OT) systems[1]. While these technologies make operations more productive and efficient, they also introduce new threats and vulnerabilities that might jeopardize the safety, security, and sustainability of marine operations. Many high-profile cyberattacks on the marine sector have occurred recently, underscoring the urgent need for stronger defences and security regulations.

For instance, the shipping giant Maersk experienced a ransomware attack[2] in 2017 that affected its operations globally and resulted in a loss of $300 million, according to estimates. The NotPetya malware, which took advantage of a weakness in the organization's IT systems and quickly propagated to other systems over the network, was blamed for the attack. Another illustration is the 2018 attack on the Port of San Diego[3], which affected users' and stakeholders' access to and availability of the port's IT systems and resulted in delays and inconveniences. An employee was deceived into providing their login information via a phishing email, which was then used to gain access to the port's network and conduct the attack. These and earlier cyberattacks on the marine industry have shown the serious effects and repercussions of such occurrences on the sector and society at large. They have also highlighted the cybersecurity defences of shipping companies' weaknesses and shortcomings, which must be addressed to reduce risks and improve the sector's resilience.

The primary objective of this thesis is to offer a thorough and useful overview of the risks that affect IT and OT systems on ships, as well as the protection measures and security controls that may be used to lessen these risks. The BIMCO Guidelines on Cyber Security Onboard Ships, which offer a framework for the cybersecurity management of ships and other maritime infrastructure, will serve as the foundation for the thesis. The goal of the thesis is to assist maritime stakeholders, such as shipowners, operators, managers and other interested parties, in developing policies and practices that are efficient and long-lasting with regard to cybersecurity. Additionally, the thesis will offer suggestions and optimal procedures based on an analysis and best practices of maritime cybersecurity as well as the lessons acquired from earlier incidents and attacks.

The motivation for this thesis is the pressing need to secure maritime operations against cyber threats that could disrupt shipping, endanger crew, and compromise cargo. The maritime industry is the lifeblood of global trade, and the increasing integration of IT and OT systems into vessels has introduced new vulnerabilities. Given the limited research available in this domain, inadequate cybersecurity in the maritime sector poses substantial economic and safety risks. This study aspires to enhance the resilience of the maritime industry, promoting its safety and security.

To sum up the aforementioned analysis, the marine sector's increasing reliance on technology and automation has given rise to new cybersecurity risks that might have a major impact on the sector. The marine industry's examples of cyberattacks show the potential financial, reputational, and safety implications linked to these threats. In order to mitigate these risks and guarantee the ongoing safe and effective operation of international trade and transportation, there is a clear need for increased research and attention to be paid to cybersecurity in the marine industry. In this thesis, the critical aspects of cybersecurity in the maritime industry are explored. It aims to contribute to

safeguarding the maritime sector from emerging cyber threats and vulnerabilities, ensuring the security of vessels and the industry’s overall integrity.

The thesis is structured as follows: In Section 1, an overview of connectivity components in a vessel is provided. Section 2 delves into IT and OT systems in the maritime industry, covering their definitions, cybersecurity challenges, and differences in requirements. Section 3 presents BIMCO's Maritime Cybersecurity Guidelines, including an analysis of threat actors, vulnerabilities, and protection measures. Section 4 explores real-world IT and OT threats and protection measures, while Section 5 discusses best practices for onshore and onboard operations. Finally, Section 6 summarizes the key findings and recommendations.

To contribute to a safer and more resilient maritime industry, this thesis covers the following key aspects:

- Analysing cyber security challenges in the maritime industry
- Exploring BIMCO's maritime cybersecurity guidelines
- Investigating threats and vulnerabilities in IT and OT systems onboard ships
- Proposing best practices for improving cyber security in both onshore and onboard maritime operations

1.1 Connectivity Components of a Vessel

The connectivity of maritime vessels has increased more than ever as technology progresses. Although it enables effective and secure operations, system integration also offers substantial cybersecurity concerns. According to Mission Secure[4], the following are the numerous connectivity systems aboard contemporary marine boats, the vulnerabilities they could encounter, and the precautions that can be taken to reduce these risks.

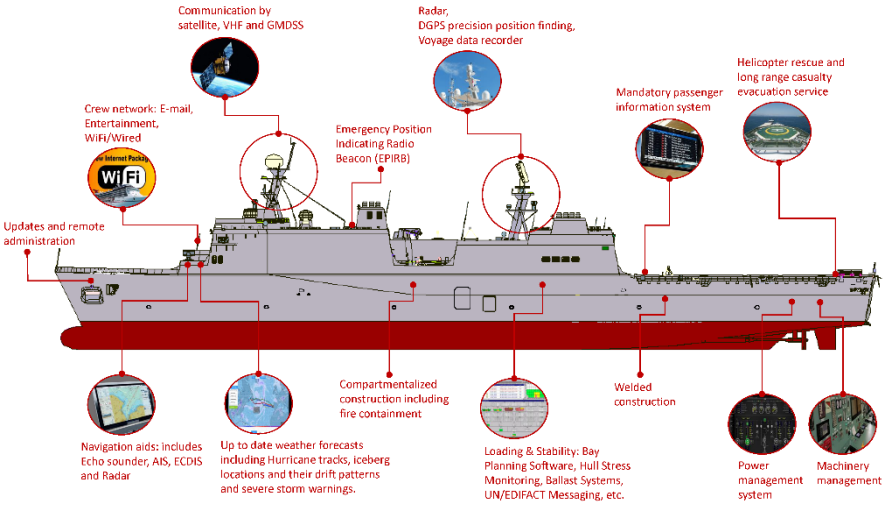

Figure 1. Automation systems of a modern ship[5]

Bridge Control Systems

For the ship to be navigated safely, the bridge systems are essential. Bridge control systems must include[6] automated identification systems (AIS), voyage data recorders (VDR), and automatic radar plotting aids (ARPA). While VDR saves all communications and data from various sensors aboard, AIS is used to track and interact with other nearby vessels. The crew of the vessel has a clear view of the surroundings thanks to ARPA's usage of radar. These systems are prone to cyber-attacks, though, and any breach might jeopardize the safety of the ship because an attacker may alter AIS data or shut down the ARPA system.

Propulsion & Power Systems

Any ship's propulsion and power systems are its vital components, and they significantly rely on digital control technologies. These systems include steering, fuel management, engine control, and onboard equipment monitoring. A cyber-attack on these systems might lead to fuel leaks, steering issues, or engine failure, all of which pose serious safety risks to the ship and its crew members.

Navigation Systems

For a vessel to safely arrive at its destination, navigation systems are essential. These systems consist of radar, weather system monitoring, GPS/GNSS, and electronic chart display and information systems (ECDIS). Electronic charts are used by ECDIS to deliver precise and up-to-date data on the position and course of the vessel. The crew can

prevent dangerous weather situations by monitoring weather systems. A cyber-attack on navigation systems could lead to incorrect positioning information or inaccurate weather data. This consequently can lead to navigation errors that could cause a collision or grounding.

Loading & Stability Systems

For a vessel to be secure and safe throughout voyage, loading and stability systems are crucial. Ballast systems, hull stress monitoring, stability control, stability decision support systems, and cargo management systems are some of these systems. Any weakness in these systems might cause the cargo to move or the vessel to capsize, both of which would have disastrous effects.

Operations Security Systems

Electronics, digital and analog sensors, programmable logic controllers, human-machine interfaces (HMI), and sensors are all components of operations security systems. These systems make sure that the equipment and systems on the ship are operating properly. A cyberattack on these systems might cause equipment to fail, resulting in reduced productivity and perhaps putting at risk the safety of the vessel.

Network Security Systems

Firewalls, segmentation tools, antivirus programs, software updates, and vendor patches are examples of network security solutions. These devices guard the ship's network backbone and shield vital systems from unauthorized access. Any breach in network security has the potential to expose sensitive information, transmit malware, or compromise vital systems.

Physical Security Systems

Server rooms, access control, bridges, mechanical spaces, and network infrastructure are examples of physical security systems. Critical infrastructure is safeguarded by these technologies, which also make sure that only authorized individuals may access sensitive systems. Any weakness in physical security might provide intruders access to private networks or adversely impact vital infrastructure.

Ship Networks

Email, customs and immigration, personnel administration, maintenance and spares management are all part of ship networks. Any vulnerability might cause serious operational interruptions because these systems are crucial to the ship's effective functioning.

Safety Systems

Fire and flood protection, tracking, shipboard security, CCTV, and emergency shutdown are all examples of safety systems. In an emergency, these systems are protecting the crew and the ship. Any malfunction of the safety systems could compromise the crew's and ship's safety.

Communications Systems

Satellite internet communications, ship-to-shore and ship-to-ship radios, portable radios, and voice-over-IP (VoIP) are examples of communication systems. Communication between crew members and between the ship and the land must be maintained by means of these technologies. Any disruption of these systems might result in a communication breakdown, making it impossible to plan emergency actions or carry out necessary tasks.

Crew Network Systems

Email, Wi-Fi, Ethernet, and bring your own device (BYOD) are just a few of the crew network systems. In order for crew members to stay in touch with their loved ones while at sea, these devices are crucial. These technologies, however, also present serious cybersecurity issues[7] since they may be exploited to gain access to private vessel systems or infect the network with malware.

Supply Chain Systems

Systems for managing vendors' updates, maintenance, and administration might be offshore or remotely. These systems make sure that the ship's technology is up to date and maintained, but they also present serious cybersecurity concerns. Any vendor upgrades or maintenance procedures could endanger crucial equipment or bring malware onto the vessel's network.

The following table provides a comprehensive overview of the vulnerable systems within a vessel that are potential targets for cyber-attacks, along with the corresponding cyber-attack types, their underlying reasons, and the potential impact.

Systems	Cyber-Attacks	Reason	Impact
Bridge Control Systems	• Unauthorized access • Spoofing or tampering • DoS/DDoS attacks	• Lack of strong authentication measures • Outdated software • Compromised networks	• Navigation errors • Accidents
Propulsion & Power Systems	• Unauthorized access • Malware / Ransomware	• Insufficient network segmentation • Weak access controls	• Loss of control • Immobilization of the vessel
Navigation Systems	• Spoofing • Malicious firmware • Interference	• Lack of encryption • Weak signal authentication	• Navigation errors • Collision risks
Loading & Stability Systems	• Unauthorized access • Data Manipulation	• Inadequate access controls • Lack of system integrity checks	• Cargo shift • Instability • Capsizing
Operations Security Systems	• Unauthorized access • Social engineering	• Lack of cybersecurity awareness	• Data breaches

Network Security Systems	• DoS/DDoS attacks • Man in the middle attacks	• Insufficient firewall configurations • Unpatched vulnerabilities	• Data breaches • System disruptions
Physical Security Systems	• Tampering	• Poor physical access controls • Inadequate monitoring	• Compromised vessel security
Ship Networks	• Network Intrusion • Malware / Ransomware	• Lack of encryption • Weak authentication mechanisms	• Data interception
Safety Systems	• Dos/DDoS attacks	• Insufficient network resilience • Weak traffic filtering	• Safety compromises • Delayed response
Communications Systems	• Eavesdropping • Message Manipulation	• Weak encryption • Lack of message integrity checks	• Misinformation
Crew Network Systems	• Phishing • Social Engineering	• Lack of cybersecurity training • Weak email security	• Data breaches
Supply Chain Systems	• Supply Chain Attacks	• Lack of supply chain security assessments • Compromised suppliers	• Compromised components • System vulnerabilities

Table 1. Targeted Systems in Cyber Attacks - Reasons and Impact Overview

More specifically, the critical communication and control systems, as well as their vulnerabilities and consequences, are listed in the table below (Frank Akpan et al., 2022).

Systems	Vulnerabilities	Consequences
AIS	• Signal interference • False information sharing • Malware • Spoofing • No encryption • Signal jamming	• Ship hijacking • Destruction of data Theft of valuable data
ECDIS	• Obsolete Oss • Insecure update mediums	• Loss of communication with the Navigation System • Hijacking of a ship • Sensitive data theft • Compromising computers and Oss
GNSS and GPS	• Jamming attacks	• Ship hijacking

	• Weak signal strength • Interference • Spoofing attacks • DoS/DDoS attacks • Packet modification	• Problems with the Navigation System • GPS signal false information • Disrupt vessel operation • Delays in services
Radar	• Jamming attacks • Spoofing attacks • DoS/DDoS attacks	• Loss of communication with the Navigation System • Loss of lives and cargo • Delays in cargo management
Propulsion and machinery management and power control systems	• Malware attack • DoS/DDoS attacks • Smuggling • Stealing • Manipulation attacks	• Ship hijacking • Diversion of the ship • Propulsion System could be interrupted • Ship damage • Financial damage • Disclosure of sensitive data

Table 2. Ship's communication and control systems, vulnerabilities, and their consequences

2. Overview of IT and OT systems on maritime

2.1 Definition and description of IT and OT systems

The maritime industry relies heavily on IT and OT systems[8], which provide assistance and services for a range of activities like navigation, cargo management, communication, and maintenance. Networks, hardware, and software known as IT systems serve office and commercial functions including accounting, finance, and inventory management. The OT found on board ships, such as the propulsion, engines, power production, and environmental control, are governed and monitored by specialized hardware and software. These systems are designed to operate autonomously or semi-autonomously with minimum human input in order to achieve optimal performance and efficiency.

The world of maritime operations relies on a vast network of interconnected systems[9] that seamlessly collaborate to accomplish their intended objectives. Within this intricate framework, crew members and shore-based employees rely on various tools such as servers, workstations, laptops, and mobile devices to carry out their tasks, facilitating essential communication, data processing, and reporting functions. Supporting this ecosystem are vital connectivity elements like satellite links, LANs, and WANs, which establish seamless channels for real-time data exchange and communication between ships and onshore facilities. IT and OT systems in the maritime sector are becoming more linked and interdependent[10] since each system may depends on the other to work properly. For instance, the navigation system depends on the communication system to receive meteorological and navigational data, while the power management system depends on the OT system to limit power consumption in accordance with the ship's operational requirements. As a result, the security and dependability of these systems are crucial for the efficient and safe operation of ships.

2.2 Cyber security challenges in maritime

The maritime industry heavily depends on IT systems for a wide range of operations, including communication, logistics, navigation, and maintenance. These systems play a crucial role in ensuring seamless information flow between ships and onshore facilities, facilitating accurate and timely data transfer. At the same time, OT systems are vital for overseeing and managing physical systems and procedures onboard ships, prioritizing safety, reliability, and operational efficiency.

According to “Maritime Cyber Priority 2023” survey conducted by DNV[11], a significant proportion of maritime professionals predict serious consequences from cyber incidents. Specifically, 76% believe that such incidents could likely lead to the closure of a strategic waterway. Additionally, 60% anticipate that cyber-attacks could result in ship collisions and 68% see the possibility of groundings. Furthermore, 56% of these professionals even expect such incidents to potentially cause physical injury or death. Echoing these concerns, an overwhelming majority of 79% assert that the industry considers cybersecurity risks to be of equal importance to health and safety risks. Despite these data, according to the same survey, only 32% of maritime professionals agree that their organization is very well prepared for preventing direct cyber-attacks on its OT systems. The corresponding figure for IT systems is 40%.

The aforementioned survey from DNV concludes that the main cyber security challenges facing the shipping sector are those presented in the following chart.

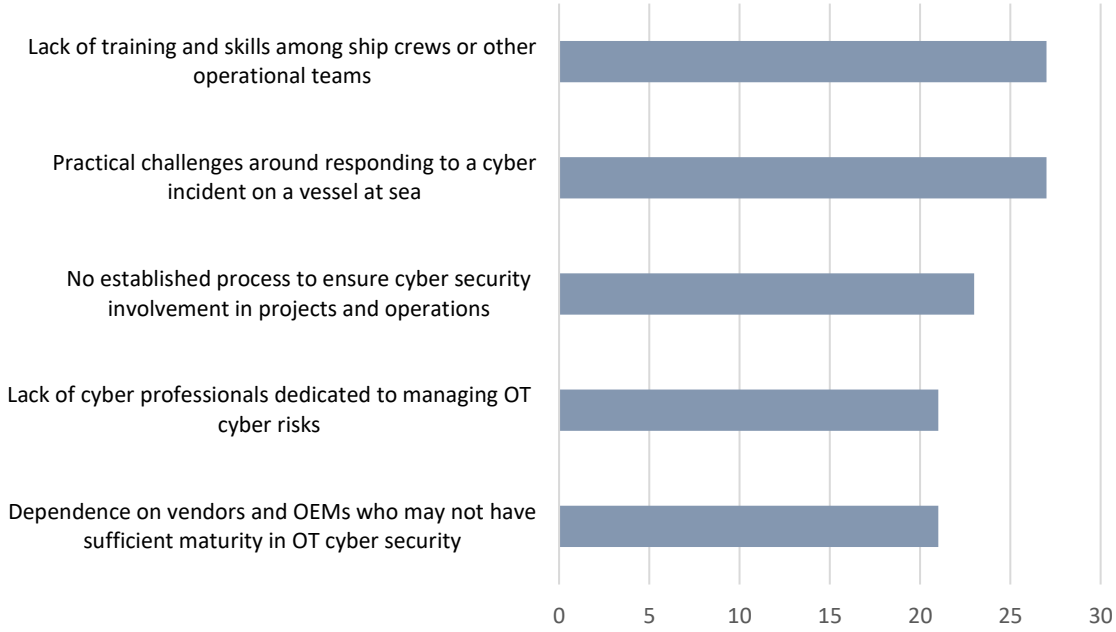

Figure 2. Percentage of the top cyber security challenges that the maritime industry faces

Although these cybersecurity challenges can guide the subsequent actions that cybersecurity professionals in the maritime industry need to undertake, the following challenges are those encountered the most within IT and OT systems on vessels, as informed by discussions with IT/Information Security personnel from numerous maritime organizations in Greece.

Challenges with IT Systems:

- Integration and Interoperability: Vessels rely on a plethora of IT systems to manage essential functions such as navigation, communication, and cargo handling. These systems can originate from different manufacturers and are expected to seamlessly integrate with each other. However, this integration is not always achieved effortlessly. Discrepancies in protocols, software versions, and hardware components frequently give rise to compatibility issues, thus creating potential vulnerabilities for malicious exploitation. Instances where essential systems fail to communicate due to integration-related complications create security gaps through which malicious actors (such as APTs mentioned in Section 3.2) can infiltrate.
- Dynamic and Unpredictable Maritime Environment: Maritime cybersecurity operates within a distinctive framework characterized by a constantly shifting and unpredictable environment. Vessels navigate through various geographical regions, contend with diverse weather patterns, and interface with disparate communication networks. These ever-evolving variables render the maintenance of a stable and secure IT environment a formidable challenge. Cyber vulnerabilities may surface or evolve rapidly, complicating timely threat detection and mitigation. For instance, when a vessel traverses regions with unreliable network access, it becomes a prime target for cyber-attacks due to the unavailability of real-time threat updates and patches.
- Lack of Cybersecurity Awareness: Despite the pivotal role played by personnel in upholding maritime cybersecurity, a notable gap exists in terms of cybersecurity awareness and comprehension among employees, contractors, and crew

members. Many individuals serving on vessels have not received formal training in cybersecurity best practices, making them susceptible to committing inadvertent security lapses.

Challenges with OT Systems:

- Bandwidth and Connectivity Limitations: Maritime vessels frequently operate in remote or offshore areas where bandwidth and connectivity options are notably constrained. These limitations pose obstacles when it comes to enhancing cybersecurity measures. Real-time monitoring and response to cyber threats become intricate endeavours when vessels find themselves distant from land-based support and communication infrastructure. The limitations in bandwidth also hinder the expeditious transmission of security updates and patches, leaving OT systems potentially exposed to cyber-attacks.
- Outdated Technology: Maritime vessels are renowned for their enduring lifespans. The aspect of this longevity also signifies a dependence on antiquated technological systems. These legacy systems, though robust, often lack the essential security features and updates found in contemporary counterparts. Securing such legacy systems against modern cyber threats represents a formidable challenge. Consequently, a proactive approach is needed, encompassing strategies to secure older systems and planning for future technological upgrades.

2.3 IT & OT Requirements and Differences

Modern ships' IT and OT systems are integrated more and more, but each of these systems has its own special requirements and characteristics. Therefore, it is essential to comprehend how these two systems differ in order to build efficient cybersecurity measures. According to Mission Secure[12], some of the differences in IT and OT system requirements include:

Performance

IT systems on ships are developed for non-real-time tasks including document management, email communications, and administrative work. The most crucial aspect of an IT system's performance is consistency, which guarantees that users can rely on it to respond consistently each time they use it. IT systems are not critical for emergency response, and their response times are not time critical. Access control is crucial for IT systems, and it is possible to establish strictly controlled access to the extent required for security. On the other hand, OT systems aboard ships are created to monitor and manage the physical operations of the ship, and real-time performance is essential for the ship to operate safely and effectively. The OT system's response time is time-critical in an emergency because it must react rapidly to human and other emergency interactions. Access control is important for OT systems as well, but it must not hinder or obstruct human-machine communication. Crew members must be able to interact with the OT system in order to monitor ship operations and address any potential problems.

Availability/Reliability

IT systems are designed to support administrative tasks and business operations, and therefore, their availability requirements can often be tolerated depending on the system’s

operational requirements. IT systems can experience short downtimes, and responses such as rebooting are acceptable. In many cases, IT systems can be rebooted or reconfigured without causing any significant impact on business operations. In contrast, OT systems bear significant cybersecurity implications as they are mission-critical and have high availability requirements. OT systems are responsible for controlling the ship's operations, ensuring the safety of the crew and the ship, and meeting regulatory requirements. As such, downtime in OT systems can have a severe impact on the ship's operations, and responses such as rebooting may not be acceptable because of operational requirements. OT systems must operate continuously without interruption to ensure the safe and efficient operation of the vessel.

Moreover, cybersecurity concerns and availability requirements may necessitate redundant systems in OT systems. The redundancy of critical systems, such as the propulsion system, ensures that the vessel can continue to operate even in the event of a system failure. In the case of OT systems, system failures carry substantial cybersecurity risks, including potential loss of life, environmental harm, and financial loss. Thus, the reliability of OT systems is of paramount importance.

Risk Management

IT systems on board ships are responsible for managing data related to various ship operations, making cybersecurity an overriding concern. The importance of data confidentiality and integrity in these systems cannot be overstated, given the potential consequences of a breach. Such breaches can severely disrupt ship operations, leading to delays in ship clearance, cargo handling, and overall business functions, thereby emphasizing the cybersecurity aspect. Furthermore, while fault tolerance may be less critical in IT systems, any significant risk event could result in substantial operational delays and far-reaching repercussions within the maritime sector.

In contrast, OT systems aboard ships are primarily focused on controlling the physical world and ensuring human safety, underscoring the importance of cybersecurity. The highest priority in OT systems revolves around human safety, closely followed by process safeguarding, underlining the pivotal role of fault tolerance. Even momentary downtime may be unacceptable due to the significant consequences that may ensue. Major risk impacts in OT systems could lead to regulatory non-compliance, environmental impacts, and harm to the crew onboard, equipment, and/or cargo. The key distinction between IT and OT systems' risk management requirements on ships hinges on the prioritization of data confidentiality in IT systems and the paramount emphasis on human safety in OT systems.

System Operation

IT systems are designed to be compatible with the most common operating systems that are widely available in the market nowadays. This implies that upgrades and maintenance of IT systems can be easily carried out with the help of automated deployment tools, making the whole process straightforward and efficient. These systems also usually have built-in security capabilities to ensure the safety and confidentiality of data. In contrast, OT systems often have differing and proprietary operating systems, which may not have built-in security features. This can create challenges when upgrading or maintaining OT systems, as specialized knowledge and tools may be required to make changes to the software. Additionally, the process of upgrading or changing the software is made more difficult by the fact that OT systems sometimes contain unique control algorithms and

updated hardware and software. The majority of the time, software suppliers that are experienced with the particular OT systems onboard the ship must carefully make these modifications.

Resource Constraints

When designing IT systems, it's important to make sure they have enough space to incorporate third-party applications, like security software. This is because these systems often use hardware that can handle different types of tasks, such as emailing, using office software, and accessing the internet. To ensure the best performance and security of these systems, they are built with the capability to add new hardware and software components. On the other hand, OT systems have certain requirements that must be considered. Because they were created to serve industrial operations, these systems might not have the memory or computing capability to facilitate the installation of security mechanisms. Any modifications or additions must be carefully considered and tested to guarantee they won't affect the system's functioning and stability since OT systems perform certain duties that are essential to the ship's overall performance. When making changes to these systems, it's necessary to proceed with caution because any disturbance might have a severe impact on their crucial function in the ship's operations.

Communications

IT systems primarily rely on standard communications protocols and primarily employ wired networks, although localized wireless capabilities may also be utilized. These networks follow typical IT networking practices and are designed to manage data effectively. In contrast, OT systems have several proprietary and standard communication protocols, and they employ various types of communications media, including radio, satellite Internet, ship to shore, ship to ship, and VoIP. The networks utilized by OT systems are complex and sometimes require the expertise of control engineers. The differences in communication requirements between IT and OT systems can be attributed to the nature of their operations. IT systems focus on business functions such as email, accounting, and other administrative tasks, and therefore their communication needs are relatively straightforward. On the other hand, OT systems are responsible for controlling and monitoring critical equipment such as engines, propulsion systems, and safety equipment, which require diverse and complex communication capabilities to ensure safe and efficient operations.

2.4 Key stakeholders and actors involved

Ship Owner – Ship Manager

In the maritime industry, the relationship between shipowners and ship managers plays a crucial role in ensuring effective cyber risk management onboard vessels. According to the "Guidelines on Cyber Security Onboard Ships"[13], the Document of Compliance (DoC)[14] holder, typically the shipowner, holds the ultimate responsibility for managing cyber risks. In cases where the ship is under third-party management, it is advised by BIMCO that, the ship manager establishes an agreement with the shipowner. This agreement should focus on delineating the split of responsibilities between the shipowner and ship manager, aligning expectations, and establishing specific instructions and requirements for the manager's involvement in purchasing decisions. It is essential to consider not only the International Safety Management (ISM) requirements but also other relevant regulations such as the General Data Protection Regulation (GDPR) and specific

cyber regulations of coastal states. To ensure clarity and commitment, written agreements between ship managers and shipowners regarding cyber risk management are recommended. These agreements serve as a foundation for open discussions on the implementation of an efficient cyber risk management, allowing both parties to work together in safeguarding the vessel's cybersecurity.

Ship owner – Agent

The relationship between shipowners and agents is of utmost importance in the maritime industry. In fact, the significance of this relationship has led to agents being recognized as a named stakeholder, engaging with shipowners, operators, terminals, port services vendors, and port state control authorities. This continuous and simultaneous interaction involves the exchange of sensitive, financial, and port coordination information. The role of the agent goes beyond that of a mere vendor, particularly in the tramp trade where shipowners often rely on a local representative, known as an independent ship agent, to act as an extension of their company. Ensuring quality standards for agents is crucial because, just like in any other businesses, agents can also become targets of cyber-attacks. Cyber-enabled crimes, including electronic wire fraud and false ship appointments, as well as cyber threats like ransomware, highlight the need for mutual cyber strategies and enhanced relationships between shipowners and agents. This collaboration is essential to effectively mitigate the risks associated with cyberattacks. Recognizing the potential vulnerabilities in the delivery of IT or OT equipment to the ship, shipowners and agents must work together to establish robust cybersecurity measures and protection protocols.

Regulators

The creation and implementation of cybersecurity standards and regulations in the marine sector is heavily influenced by regulators and classification societies. Regulators are in charge of establishing cybersecurity rules and guidelines that control the usage and operation of IT and OT systems aboard ships, including IMO and national maritime agencies. Classification societies, such as Lloyd's Register, Bureau Veritas, and DNV GL have the responsibility to confirm and certify that ships and their IT and OT systems comply to these regulations and standards.

Recently, there has been a rising focus in the maritime industry regarding the cybersecurity[15] of IT and OT systems. Stakeholders and regulators in the industry have been motivated to act in order to strengthen the security of these systems as a result of the increasing number of cybersecurity events and threats as well as the serious operational and economic consequences of these incidents. The creation and acceptance of cybersecurity standards and guidelines is one of the important actions made by regulators and industry counterparts. The IMO has developed cyber risk management recommendations that offer a framework for managing cybersecurity risks aboard ships. Risk assessment, security management, and incident response are just a few of the subjects covered in these recommendations. Various industry groups and organizations have created their own cybersecurity best practices and standards in addition to the IMO guidelines. One example is that the biggest international maritime organisation, the Baltic and International Maritime Council (BIMCO), has created a set of cybersecurity guidelines that offer useful guidance and recommendations on managing cybersecurity risk for ships.

3. BIMCO’s Maritime Cybersecurity Guidelines

In a significant stride towards enhancing cyber security in the maritime industry, BIMCO unveiled the fourth version of "The Guidelines on Cyber Security Onboard Ships" on December 23, 2020. These guidelines, meticulously curated by industry experts, address the escalating threat of cyber-attacks faced by ships in today's digital age. With the ever-increasing reliance on technology, ships are now interconnected and vulnerable to cyber intrusions. BIMCO, acknowledges the urgent need for robust cyber security measures to protect vessels, seafarers, and operations from potential disruptions. Building upon its previous editions, this latest release represents BIMCO's dedication to fortifying the maritime sector against cyber threats. "The Guidelines on Cyber Security Onboard Ships" offer practical recommendations and a comprehensive framework to safeguard vessels from malicious cyber activities. This publication serves as a valuable resource, assisting maritime stakeholders in navigating the complex landscape of cyber security. BIMCO's decision to release the fourth version of these guidelines underscores their commitment to fostering a culture of cyber resilience in the maritime community. By providing guidance and promoting risk management practices, BIMCO is at the forefront of efforts to ensure a secure digital future for the shipping industry.

3.1 Threat Actors

When it comes to maritime cybersecurity, the motives, threats, and actors play a significant role in shaping the security landscape. The maritime industry faces a range of motives that drive malicious activities, including but not limited to financial gain, disruption of critical operations, and even threats to human life. Various threat actors with different motivations pose potential risks to the cybersecurity of ships. These threat actors include accidental actors, activists, criminals, opportunists, states, state-sponsored organizations, and terrorists. Accidental actors, despite having no malicious intentions, can inadvertently cause harm by unknowingly introducing infected USB devices into the ship's IT or OT systems. Activists, including disgruntled employees, may seek revenge, disrupt operations, attract media attention, or cause reputational damage. Criminals are motivated by financial gain[16], engaging in activities such as commercial espionage or industrial espionage to steal valuable information or gain a competitive advantage. Opportunists are attracted to the challenge of breaching cybersecurity defences, as well as the potential for reputational or financial gain that may arise from successful attacks. On a more significant scale, states, state-sponsored organizations, and terrorists may have political or ideological motivations. Their objectives can range from causing controlled or uncontrolled disruptions to economies and critical national infrastructure to engaging in espionage, seeking financial gain, or conducting commercial and industrial espionage to undermine competitors. It is important for the maritime industry to be aware of these different motivations and potential risks posed by each threat actor category in order to develop robust cybersecurity measures and effectively protect shipboard IT and OT systems from cyber threats.

In recent years, the maritime sector has become an attractive target for Advanced Persistent Threat (APT) groups, posing significant cybersecurity challenges to companies operating within this sector. Analysing their tactic and techniques is essential for understanding the evolving cybersecurity landscape in the maritime industry and formulating effective defence strategies. The following table, retrieved from Hunt & Hackett[17], presents an overview of notable APT groups known to have engaged in cyberattacks against the maritime sector and associated organizations.

Origin Country	Actor
China	• APT1 • APT10 • APT12 • APT15 • APT17 • APT19 • APT21 • APT26 • APT40 • APT41 • Blue Termite • Earth Lucca • Earth Wendigo • Ice Fog • Lucky Cat • Microcin • Night Dragon • POISON CARP • RedAlpha • Red Delta • RedEcho • Suckfly • TA530 • TaskMasters
Iran	• APT35 • APT39 • CHRYSENE • COBALT CATANA • Cutting Kitten • Fox Kitten • IRIDIUM • LYCEUM • Madi • MuddyWater • Tortoiseshell
Russia	• APT28 • APT-C-34 • CIRCUS SPIDER • ELECTRUM • FIN7 • Gamaredon Group • Inception Framework • Operation BugDrop • TeamSpy Crew • TEMP.Veles
North Korea	• APT38 • Kimsuky • Wassonite
Kazakhstan	• Fxmsp • Operation Manul
Vietnam	• APT32
Colombia	• APT-C-36
India	• Dark Basin
Lebanon	• Dark Caracal
Libya	• Libyan Scorpions
Palestinian Territory	• Molerats
Saudi Arabia	• OurMine
Ukraine	• Operation Groundbait
United Arab Emirates	• Stealth Falcon
United States	• Equation Group

Unknown	• FIN10 • FIN8 • Honeybee • MUMMY SPIDER • Operation Ghoul • Operation Parliament • Orangeworm • RedCurl • SWEED • TA2101 • TA2722 • WildNeutron • WildPressure • ZooPark

Table 3. Attack groups targeting the maritime sector and their country of origin

3.2 BIMCO's Analysis of Cybersecurity Vulnerabilities in the Maritime Industry

According to BIMCO, onboard maritime vessels, both existing and newbuild ships, several common cyber vulnerabilities can be found. These vulnerabilities expose the vessels to potential cyber threats and compromise their cybersecurity posture. One such vulnerability is the presence of obsolete and unsupported operating systems, which lack the necessary security updates and patches to address emerging threats. Additionally, ships may have unpatched system software, leaving them susceptible to known vulnerabilities that can be exploited by attackers. Another critical vulnerability is the absence of updated or missing antivirus software and malware protection. Without robust and up-to-date security solutions, ships are more susceptible to malware infections and other malicious activities. Inadequate security configurations and best practices further exacerbate the situation, including ineffective network management and the continued use of default administrator accounts and passwords. Such practices provide easy entry points for attackers to gain unauthorized access to systems and networks.

Furthermore, shipboard computer networks often lack essential boundary protection measures and proper segmentation. The absence of these safeguards allows unauthorized access and lateral movement within the network, potentially compromising critical systems and sensitive data. Additionally, safety-critical equipment or systems that remain connected to the shore side pose inherent risks as they provide potential entry points for attackers to infiltrate onboard systems. Inadequate access controls for third parties, including contractors and service providers, represent another vulnerability. Insufficient measures to manage access to cyber assets and networks create opportunities for unauthorized individuals to gain access and exploit vulnerabilities. Moreover, the lack of comprehensive training and skills among the vessel's staff to manage cyber risks leaves them ill-equipped to identify and respond to potential threats effectively.

Lastly, the absence, inadequacy, or lack of testing of contingency plans and procedures is a vulnerability that can hinder effective response and recovery in the event of a cyber incident. A robust and tested plan is essential to mitigate the impact of cyber-attacks and ensure the vessel can swiftly and effectively restore normal operations. Addressing these vulnerabilities requires a holistic approach, encompassing regular system updates, robust security configurations, effective access controls, comprehensive training programs, and well-defined contingency plans.

Summary of Vulnerabilities

- obsolete and unsupported operating systems
- unpatched system software
- outdated or missing antivirus software and protection from malware
- inadequate security configurations and best practices, including ineffective network management and the use of default administrator accounts and passwords
- shipboard computer networks, which lack boundary protection measures and segmentation of networks
- safety critical equipment or systems always connected with the shore side
- inadequate access controls to cyber assets, networks etc for third parties including contractors and service providers
- staff inadequately trained and/or skilled to manage cyber risks
- missing, inadequate or untested contingency plans and procedure

Despite the rising cyber incidents and the preceding vulnerabilities, there is a lack of a structured approach to effectively manage maritime cyber risks. The insurance industry is exploring ways to cover cyber-physical risks[18] but faces challenges[19] in estimating such risks, resulting in coverage gaps. The SECONDO[20] platform acts as a solution to optimize cyber insurance premiums, bridging the gap between insurers and the insured where underreporting of cyber incidents fosters a deceptive sense of security. Moreover, even though cyber insurance companies offer a range of coverage options, understanding contract terms and comparing offerings can be daunting for customers[21].

3.3 BIMCO's Defence Approach

The defence approach that BIMCO's guidelines suggest, is to follow the principles of defence in depth and in breadth.

Defence in depth

Protecting critical systems and data in the maritime industry requires a comprehensive approach that takes into account the role of personnel, procedures, and technology. Implementing multiple layers of protection measures is crucial to enhance the detection of cyber incidents and safeguard the confidentiality, integrity, and availability of data in both IT and OT systems. When it comes to connected OT systems on board, relying solely on perimeter defences like firewalls may not be enough to address the diverse range of threats, including insider risks. Therefore, a defence in depth strategy is recommended, which combines various measures to ensure comprehensive protection.

This defence in depth approach includes several components such as physical security in line with the ship security plan (SSP), network protection with effective segmentation, intrusion detection, firewall implementation, regular vulnerability scanning and testing, software whitelisting, access and user controls, configuration and change management controls, proper handling of removable media, and robust password policies. Furthermore, personnel's awareness and understanding of cybersecurity risks are crucial. It is important for individuals within the maritime industry to be well-informed about cybersecurity best practices and to understand the potential risks they may encounter. Adequate training and familiarity with appropriate procedures, including incident response

protocols, are essential elements of a comprehensive cybersecurity framework. Incorporating cybersecurity into company policies and procedures ensures that it is considered as an integral part of the overall approach to safety and security risk management. Given the complexity and persistence of cyber threats, adopting a "defence in depth" mindset is vital.

Defence in breadth

When it comes to developing integration between systems on maritime vessels, it is crucial to establish a trust boundary model. This model involves grouping systems based on implicit trust, such as user workstations, and explicit trust, such as the connection between bridge computers and corporate networks. For larger or more complex networks, it is essential to engage in threat modelling to identify areas where technical controls should be implemented between systems. This approach supports a defence in breadth strategy, ensuring a wide range of protective measures are in place.

Onboard ships, where the integration between IT and OT systems can be extensive, defence in depth alone is not sufficient. It is crucial to adopt a defence in breadth approach, which involves implementing technical and procedural protection measures across all vulnerable and integrated systems. The aim is to prevent vulnerabilities in one system from being exploited to bypass the security measures of another system. Defence in depth and defence in breadth are complementary approaches that, when implemented together, form the foundation of a holistic response to managing cyber risks. The implementation of cybersecurity controls should be prioritized, giving attention to measures or combinations of measures that offer the greatest benefits. While it is important to protect all systems, it is necessary to consider the cost and effort required, as in some cases, the investment in time and resources may outweigh the actual risk of infection itself. By adopting a trust boundary model, conducting threat modelling, and applying defence in depth and breadth principles, maritime vessels can establish a robust cybersecurity framework that safeguards their integrated systems and mitigates the potential risks posed by cyber threats.

3.4 BIMCO’s Protection Measures

3.4.1 Technical Protection Measures

Limitation to and control of network ports, protocols and services

In order to maintain a secure network environment, it is crucial to establish limitations and control over network ports, protocols, and services. This can be achieved through the implementation of access lists, which serve as a means to enforce the company's security policies. By carefully configuring access lists, organizations can ensure that only authorized and appropriate traffic is allowed through their networks or subnets, aligning with the specific control policies in place. Furthermore, BIMCO highlights the importance to take necessary measures to secure routers against potential incidents and threats and

proceeds by stating that one effective step is to close unused ports. This control significantly reduces the risk of unauthorized access to critical systems or sensitive data.

Configuration of network devices such as firewalls, routers and switches

When considering the connectivity of systems on maritime vessels, it is crucial to assess whether they should be attached to controlled or uncontrolled networks. Controlled networks are specifically designed to mitigate security risks through the implementation of firewalls, security gateways, routers, and switches. These networks provide a higher level of security, safeguarding critical systems necessary for the operation of the ship itself. Additionally, networks that allow suppliers remote access to navigation and other OT systems onboard should also be controlled. While it may be necessary to grant suppliers access for system upgrades or remote servicing, it is essential to secure the shoreside external access points to prevent unauthorized entry.

Certain systems such as cargo stowage, load planning, container management, and mandatory ship reporting systems should also be included within the controlled network. These systems are critical to ensuring efficient operations and compliance with regulatory requirements. On the other hand, there are networks that can be considered uncontrolled. These networks are typically associated with guest access, passenger recreational activities, or providing private internet access for the crew. It is important to note that any wireless network should generally be regarded as uncontrolled due to the inherent risks associated with wireless communication.

The segregation between controlled and uncontrolled networks is necessary to minimize the potential risks posed by uncontrolled networks. Uncontrolled networks may lack data traffic control, making them highly vulnerable to malware infiltration. Therefore, it is crucial to isolate uncontrolled networks from the controlled ones, especially when direct internet connectivity is involved. By carefully determining which systems should be attached to controlled or uncontrolled networks, maritime vessels can enhance their cybersecurity posture and ensure the integrity and reliability of critical operations while mitigating the risks associated with uncontrolled network environments.

By implementing well-designed segregation measures, the accessibility of a ship's systems to potential attackers can be significantly hindered, serving as a highly effective technique in impeding the spread of malware. To achieve this, onboard networks should be carefully partitioned using firewalls, creating distinct safe zones. It is essential to regularly review and monitor firewall configurations to promptly identify any unauthorized changes. By minimizing the number of communications links and devices within each zone, the overall security of systems and data within that zone can be heightened. Moreover, it is prudent to place confidential and safety-critical systems within the most protected zone, further reinforcing their security measures.

Several vendors, such as Marpoint and Marel Navigation and Communication, offer vessel-targeted solutions for the secure configuration of network devices. Marpoint has developed the Evo2 Router[22], an enterprise-grade multi-WAN network management solution designed for seamless internet connectivity that is independent of the airtime provider. The router supports multiple satellite bands and provides advanced network management capabilities, including the creation and management of access rules. These

rules can be configured to restrict network access based on user roles and device types, thus improving network security and preventing unauthorized access.

Notably, the Evo2 Router also comes equipped with a control panel that enables direct administration, making it easier to monitor and manage various elements of the vessel's network infrastructure, such as network performance, bandwidth usage, data consumption, and speed. The router's detailed logging and alerting system also enables maritime organizations to track network usage and detect any unusual activity, thereby providing an added layer of security. Additionally, the Evo2 Router can be integrated with Marpoint's Network Asset Management platform, which provides a centralized view of the network and helps IT teams to monitor, track, and control their assets. When the Evo2 Router is installed, it automatically discovers all the assets on the vessel's network and documents them in the network asset management platform, thus saving time and effort for IT teams. Key features of the Evo2 Router include an enterprise-grade firewall, effective network segmentation, DNS and application filtering, multi-WAN with auto-gateway selection and load balancing.

Another vendor is Marel Navigation and Communication that offers a turn-key communication solution[23] that includes the supply and customization of branded firewalls to improve the security and operational efficiency of the vessel's network. In partnership with Fortinet[24], Marel's network engineers are trained to configure the firewall devices to match the demanding maritime organization's operational needs. Specific tasks related to firewall configuration include the creation of virtual local area networks (VLANs) for different user groups, defining security rules for each user group and managing load balancing and/or failover for multiple WANs.

Physical security

In the context of cybersecurity, physical security serves as a vital line of defence. Physical security[25] refers to the measures in place to secure ship systems from physical attacks or unauthorized access. Physical security can be compromised through poor access controls, inadequate security measures, or social engineering attacks. While it may seem simple and obvious, it is an essential aspect of managing cyber risks effectively. Implementing a comprehensive defence strategy requires a focus on physical control measures that cannot be easily bypassed. Critical areas housing sensitive OT and IT control components should be securely locked, ensuring that unauthorized individuals cannot gain access. Furthermore, it is crucial to safeguard security and safety-critical equipment and cable runs from any unauthorized interference. Even seemingly minor details like securing physical access to sensitive user equipment, such as USB ports on bridge systems, play a significant role in bolstering overall cybersecurity defences.

Gaining physical access to a ship's network and systems poses a significant threat as it can lead to cyber-attacks. To mitigate such risks, various protection measures can be implemented. One approach is to implement access control policies that limit physical access to critical systems to authorized personnel only. Additionally, regular physical security audits can be conducted to ensure the effectiveness and up-to-dateness of the physical security measures. Furthermore, implementing physical security measures, such as CCTV cameras, intrusion detection systems, access control systems, and physical barriers, can prevent unauthorized access to critical systems.

Research conducted by Ahonen (2020)[26] on cyber security of highly automated connected machines, highlights the importance of utilising Hardware Security Module (HSM) and Trusted Platform Module (TPM) to introduce an additional layer of security. HSMs[27] serve as specialized cryptographic processors dedicated to protecting the cryptographic key lifecycle. These trust anchors are meticulously designed to protect the cryptographic infrastructure by securely managing, processing, and storing cryptographic keys in an impenetrable, tamper-resistant device. HSMs are renowned for their ability to enhance security by fortifying critical operations, including encryption, decryption, authentication, and digital signing, making them indispensable tools for protecting transactions, identities, and applications. Complementary, TPM[28] constitutes a specialized computer chip (microcontroller) explicitly designed for the secure storage of critical components used to verify the integrity of a computing device. These elements encompass a spectrum of sensitive data, ranging from passwords and certificates to encryption keys. Furthermore, TPMs play a pivotal role in preserving platform integrity by recording platform measurements. These measurements, in turn, are instrumental in substantiating the platform's trustworthiness. TPMs facilitate two fundamental processes: authentication, which verifies the platform's claimed identity, and attestation, a mechanism crucial for demonstrating that a platform maintains its integrity and remains uncompromised.

Satellite and radio communication

Ensuring the cybersecurity of radio and satellite connections requires a collaborative effort with service providers. When establishing requirements for onboard network protection, it's crucial to take into account the specifications of the satellite link. Typically, a satellite terminal has an unprotected LAN port for connecting to the ship's networks, presenting various options for protection based on the specific threats. Protection against eavesdropping often involves establishing a VPN connection or using encrypted protocols. On the other hand, safeguarding against intrusion and unauthorized access can be achieved through different means, such as collaborating with the service provider to implement a security arrangement, establishing a connection through a secure server ashore (owned by the company), or employing an onboard firewall. An important aspect of cybersecurity is making the satellite terminal invisible and less susceptible to unauthorized access. This can be accomplished by deactivating certain functions like the "remote administration page" and "port forward" in the terminal's settings menu. When establishing connections between a ship's navigation and control systems and shore-based service providers, preventing unauthorized access to onboard systems is of high importance. It is advised not to publish a public IP address that is directly routable to the ship from the internet. Instead, connections from the internet should be routed through a shoreside network and firewall to ensure proper routing and access control. Additionally, closely monitoring outbound connections originating from ship networks, control networks, or networks with connections to control networks (such as reverse tunnel connections) is another critical consideration.

To ensure a robust and secure network environment, several measures should be implemented when utilizing a VPN for maritime communication. First and foremost, it is crucial to encrypt the data traffic to meet international encryption standards[29]. This encryption safeguards the confidentiality and integrity of the transmitted information,

making it unreadable to unauthorized individuals. Additionally, deploying a firewall as a protective barrier in front of servers and computers connected to the networks, whether onshore or onboard, is essential. The firewall acts as a filter, monitoring and controlling incoming and outgoing network traffic, blocking potentially malicious or unauthorized access attempts. Choosing the appropriate routing and connection type for specific traffic is another vital consideration, and expert guidance from the distribution partner can greatly assist in making informed decisions. Onshore filtering of traffic, involving the inspection and potential blocking of data packets, is a collaborative effort between the shipowner and the distribution partner. Combining this onshore filtering with firewalls and security inspection/blocking gateways onboard the vessel ensures a comprehensive and layered approach to protection. These measures complement each other, collectively forming a strong defence against potential cyber threats.

When it comes to satellite communication terminals and other communication equipment, manufacturers often provide management interfaces with security control software. These interfaces, commonly accessible over the network through web-based user interfaces, require special attention to ensure their protection. An assessment of a ship's installation should include evaluating the security measures applied to these administrative interfaces. To enhance security, access to these interfaces can be restricted to specific networks, limiting the potential attack surface. Furthermore, unnecessary interfaces that are only used during initial configuration can be disabled entirely, minimizing potential vulnerabilities. Additionally, managing passwords appropriately is crucial. Default passwords, which are often well-known to cybercriminals, should be changed to unique, strong passwords to prevent unauthorized access and unauthorized configuration changes.

Orange Business Services, a global integrator of communications products and services, has developed an integrated solution named "Maritime Connect"[30] for the maritime industry that addresses the critical concern of maritime cybersecurity, specifically focusing on satellite and radio communication. Maritime Connect functions as a platform that facilitates the seamless integration of ships into the corporate network. It is compatible with any satellite system, including Very Small Aperture Terminal (VSAT), and is able to provide both voice and data services to crew and passengers. The services it offers are similar to terrestrial networks, with the differentiation largely arising from the outdoor technology deployed to accommodate the mobility and the sea conditions that characterize maritime operations. Notably, the entire solution is self-contained in a single, onboard-installable box, thereby enhancing its feasibility and ease of implementation. The platform also extends Business VPN over the sea, which supports mission-critical applications. Maritime Connect is structured to provide reliable connectivity to all maritime satellite networks, thus enabling swift adaptability to the changing needs of the maritime industry. In terms of security, Maritime Connect provides applications that ensure onboard security at all times, in addition to features like private network, multiple access, and private cloud connectivity.

Wireless access control

To ensure secure wireless access to networks aboard ships, it is crucial to implement robust measures that restrict access to authorized devices and employ strong encryption

keys that are regularly updated. Several considerations can help in effectively controlling wireless access. One approach is to utilize enterprise authentication systems that employ asymmetric encryption, while also isolating networks using dedicated access points. This allows for the segregation of guest networks from administrative networks, enhancing security. Additionally, deploying wireless intrusions prevention systems (IPS) can help intercept unauthorized access points or rogue devices, bolstering network protection. Network Access Control (NAC) can be employed to profile devices, distinguishing between corporate and personal devices, and enabling effective management of wireless network access. It is also important to safeguard the physical interconnection points between wireless access devices and the network, such as network plugs and racks, to prevent unauthorized access by rogue devices.

Antamedia offers a commercial solution[31] for wireless access control. This solution prioritizes reliability and control. The system operates by integrating with Wi-Fi hardware located on each vessel, controlling Wi-Fi usage. While docked, the Wi-Fi system uses the port's Wi-Fi connection. Upon leaving the port, the system can switch to 4G/5G connections within range. When at sea and out of range of terrestrial networks, the connection fails over to satellite. This flexible and adaptive approach ensures continuous connectivity, vital for maritime operations. Antamedia's Maritime Wi-Fi system offers an array of features that contribute to its utility and effectiveness in managing cybersecurity in a maritime context such as access controls and web filtering. It also features options for automatic user login, and real-time statistics and usage reports. This system can be managed remotely, which is crucial for operations distributed across different geographical locations. From a central management perspective, Antamedia's system can be controlled from any device, anywhere. This feature enhances its suitability for maritime operations, where centralized control and monitoring are essential.

Secure configuration of hardware and software

In order to enhance cybersecurity measures, it is crucial to restrict user profiles within the maritime industry to ensure that computers, workstations, or servers are solely utilized for their designated purposes. By implementing user profile restrictions, it becomes possible to prevent users from making unauthorized alterations to systems or installing and running new programs. This approach helps mitigate the risks associated with inadvertent or intentional misuse of resources and reduces the potential for introducing vulnerabilities into the network. By maintaining strict control over user profiles, organizations can establish a more secure computing environment that aligns with their specific operational requirements and safeguards against unauthorized modifications or installations that could compromise the integrity and functionality of critical systems.

Kongsberg offers a Remote Configuration solution[32] for secure hardware and software configuration in maritime environments. The service utilizes a specialized Remote Support software and hardware that can be installed onboard, facilitating real-time collaboration between Kongsberg Maritime's global pool of service and support experts and the onboard personnel. This configuration ensures that all involved parties have a comprehensive understanding of the challenges that need to be addressed and how to implement solutions. The service kit, which includes a pre-programmed router, malware protection computer, and software for the operator stations, can be installed on a variety

of hardware platforms. Configuration tasks are carried out by certified Kongsberg engineers, following a cooperative risk assessment and remote safe job analysis between the maritime organization and Kongsberg.

The implementation of Remote Configuration Service offers a plethora of benefits that significantly enhance maritime operations. Primarily, it enables efficient technical support and service delivery for vessels in regions where the accessibility of service engineers may be restricted. This efficiency is further manifested in the form of operational support and guidance that bolsters the troubleshooting, assessment, and rapid resolution of issues associated with remote configuration. Additionally, the service provides an expedited response in instances of downtime through the immediate provision of expert assistance, directly connecting to the vessel. The service also facilitates improved preparation for service visits by providing real-time status updates and diagnostics from the systems, contributing to an optimised service experience. The provision of operational assistance during critical and complex operations further exemplifies the service's efficacy. Moreover, the Remote Configuration Service incorporates periodic inspection for preventive maintenance, enhancing the longevity and reliability of maritime systems. Lastly, the service protects installations from malware, effectively reducing potential downtime and enhancing the cybersecurity posture of the vessel.

Email and web browser protection

To safeguard both shoreside and onboard personnel from potential social engineering attacks and the unauthorized acquisition of sensitive information, it is crucial to implement robust email and web browser protection measures. Social engineering[33] refers to any technique that involves manipulating people into divulging sensitive information or taking actions that compromise ship systems. Social engineering attacks can be particularly effective in the maritime industry, where crew members may be less aware of cybersecurity risks. More specifically, phishing[34] is a social engineering technique that involves sending fraudulent emails or messages to trick recipients into revealing sensitive information or clicking on links that install malware. Phishing attacks can be particularly effective in the maritime industry, where crew members may not have extensive training in cybersecurity. To prevent social engineering attacks, various protective measures can be adopted.

First, crew members can be educated about the dangers of social engineering and trained to recognize its various forms. Security awareness training can teach employees to recognize social engineering tactics and to avoid falling victim to them. Employees should be trained to verify the authenticity of requests for sensitive information and to report suspicious behaviour to security personnel. The more effective solution is cybersecurity awareness and training that can educate employees on how to recognize and avoid social engineering tactics, reducing the likelihood of a successful attack.

Additionally, email filters can be implemented to block suspicious messages, limiting the risk of unauthorized access to sensitive information. Email filtering and anti-phishing software can detect and block emails containing malicious links or attachments. These tools can also prevent phishing attacks by verifying the authenticity of emails and warning users of potential threats.

Access controls and user privilege limitations can also be used to prevent unauthorized access to critical systems. Access controls can limit the amount of sensitive information that employees can access. This can prevent attackers from using social engineering tactics to obtain sensitive information from employees who have access to it. Multi-factor authentication is another effective protective measure, as it makes it more difficult for unauthorized individuals to gain access to sensitive data. Lastly, user activity should be regularly monitored for any suspicious behaviour that could indicate a social engineering attack. The implementation of these protective measures can help to mitigate the risk of social engineering attacks and ensure the safety and security of sensitive information.

These measures aim to prevent email-based security breaches and ensure the confidentiality and integrity of data exchanged via email or voice communications. Implementing encryption protection can effectively safeguard sensitive information during transmission. Furthermore, it is essential to deploy security measures that prevent web browsers and email clients from executing malicious scripts, thereby reducing the risk of malware infiltration. Adhering to best practices, such as sending emails as encrypted or zipped files when necessary, disabling hyperlinks within the email system, and avoiding the use of generic email addresses, can further enhance the security of email transfers. Additionally, it is crucial to configure user accounts properly within the system to maintain a secure email environment.

Many vendors, such as Inmarsat and GTMaritime, offer email and web browser protection solutions for maritime organizations. Inmarsat's solution[35], Fleet Mail, is designed to meet the challenges of the remote maritime environment. It provides secure, stable, cloud-based email services that are optimised for use at sea. The system is designed to automatically switch between Inmarsat’s satellite networks, LTE, 5G, and mobile connectivity, allowing seamless operation in and out of ports. Fleet Mail's web-based interface is accessible across any device and any front-end client, allowing users to easily adapt their existing workflows and corporate protocols. Features include control over message flows, the ability to set up pro-active alerts, automate reports, and archive vessel position data and messages for up to seven years. The service also integrates advanced security features such as multi-layered detection engines to protect against malware, viruses, spam, and social engineering attacks. In terms of setup and diagnostics, Fleet Mail is designed for easy installation with a 'one-click' setup, eliminating the need for IT support or hardware. It runs on the latest Linux and Windows operating systems, which facilitates remote diagnostics and resolution by shore-based IT teams.

Another commercial solution is GTMaritime's GTMailPlus[36] that similarly offers reliable and secure maritime email services. It secures, optimises, and delivers emails in demanding conditions, working with any satellite provider. The system integrates seamlessly with any email client and ensures optimal connectivity with zero data loss. Efficient email transfer is achieved by resuming transfer from the point of interruption, saving bandwidth and reducing interruption to crew communications. GTMailPlus incorporates comprehensive security features such as protection against malware, viruses, spam, and phishing attacks with end-to-end encrypted communications. Additional layers of protection include advanced malware detection using global threat intelligence networks and a multi-layered detection engine for guarding against all known virus signatures.

Application software security (patch management)

To maintain the security of onboard systems, it is crucial to provide regular security updates and develop a roadmap for software and hardware patching. Unpatched software[37] refers to any software that has not been updated to address known security vulnerabilities. Unpatched software can leave ship systems vulnerable to attack, as attackers can exploit known vulnerabilities to gain access to ship systems. The aforementioned updates should be integrated into the periodic maintenance cycle, with special attention given to firewalls and equipment involved in VLANs. By applying updates and patches correctly and in a timely manner, vulnerabilities in the system can be addressed before they become targets for hackers. However, patching certain OT systems can be challenging and costly. It requires aligning software and hardware firmware while conducting thorough post-installation tests to ensure system integrity. In some cases, security patches may not be applicable without partially or completely upgrading system hardware. Consequently, OT systems are not frequently updated or may not receive updates at all. It is essential to assess compatibility and potential operational impacts on OT systems before installing any patches. If a critical patch cannot be installed, alternative measures must be considered to prevent vulnerabilities from being exposed in larger IT networks or the internet. These measures could include physical protection, restricting network access, and implementing virtual patching techniques.

To avoid vulnerabilities arising from unpatched software, a number of protective measures can be adopted. For instance, patch management systems may be deployed to guarantee that software receives the latest security patches. A patch management process involves identifying software vulnerabilities and applying security patches or updates to fix them. This can be done manually or through automated patch management tools. Additionally, monitoring software vulnerabilities and prioritizing patching for critical systems can enhance security. Vulnerability scanning tools can scan computer systems and networks for unpatched software vulnerabilities. These tools can help identify vulnerable software and prioritize patching efforts. Further, educating crew members about the significance of software updates and the dangers posed by unpatched software is crucial. Patch management solutions can automate the process of updating software and ensuring that systems are running the latest version with the latest security patches.

Marpoint offers a comprehensive range of managed IT services[38], one of which is the Application Software Security, specifically patch management. The company is focused on providing a holistic approach to IT Managed Services, aiming to deliver advanced and mature technology to remotely manage and monitor the complete vessel's IT infrastructure. As part of this service, Marpoint hosts vessel applications in a virtual environment while also maintaining real-time monitoring of critical devices and assets. This includes the provision of customized software patching services, an integral part of maintaining application software security. This process allows maritime organizations to stay updated and secure by applying patches to their software systems promptly and efficiently, aiding them in compliance with the IMO 2021 Regulation[39].

3.4.2 Procedural Protection Measures

Training and awareness

Training and awareness have a vital and key role in effectively managing cyber risks, as emphasized in the guidelines. It's essential to consider the internal cyber threat, recognizing that personnel have a crucial responsibility in safeguarding IT and OT systems. However, they can also be unwittingly careless, such as transferring data between systems using removable media without taking precautions against malware transmission. To address this, training and awareness programs should be tailored to different personnel levels. This includes onboard personnel, such as the Master, officers, and crew, as well as shoreside personnel involved in ship management, loading, stowage, and operation. An onboard awareness program should be implemented based on individual roles.

The program should cover various risks, including:

Risk Category	Risk Description	Recommended Risk Mitigation Measures
Email-Related Risks	Potential for phishing emails and suspicious attachments	Educate personnel about recognizing and avoiding suspicious links and attachments
Internet Usage Risks	Risks associated with social media, chat forums, and cloud-based file storage	Raise awareness about potential risks related to less controlled and monitored data movements
Geolocation Data Risks	Risks due to publicly available geolocation data for personnel and vessels	Highlight and educate on the implications of accessible geolocation data
Personal Device Risks	Security issues arising from personal devices lacking patches and controls	Discuss the risks of using personal devices in a connected environment
Software Installation & Maintenance Risks	Threats associated with infected removable media or unauthorized software packages	Train personnel about risks and safe practices for installing and maintaining software
Software & Data Security Risks	Vulnerabilities in software and data integrity	Advocate for regular anti-virus checks, software authenticity verification, and other good security practices
User Information Risks	Potential misuse or theft of user information, passwords, and digital certificates	Encourage robust safeguarding practices for sensitive user information
Third-Party Risks	Cybersecurity threats introduced by non-company personnel	Highlight the need for strict supervision during third-party technical operations

Suspicious Activity Risks	Detection of unusual network connections or unauthorized devices	Guide personnel on identifying, reporting, and managing potential cyber incidents
Cyber Incident Impact Awareness	Consequences and impact of cybersecurity incidents on operational safety	Foster a deeper understanding of the potential outcomes of cyber incidents
Preventive Maintenance Risks	Shortfalls in implementing preventative maintenance routines	Promote implementing preventative measures, such as regular checks, patching, backups, and incident response planning and testing
Removable Media Risks	Threats posed by removable media from external service providers	Establish procedures for checking and validating removable media before connecting them to the system

Table 4. Training, Awareness and Risk Mitigation Strategies

It is crucial to ensure that personnel understands that the presence of anti-malware software does not eliminate the need for robust security procedures. This includes controlling the use of all removable media and reinforcing the importance of adherence to security protocols even with protective software in place. By providing comprehensive training and raising awareness, maritime stakeholders can enhance cybersecurity practices and mitigate potential risks associated with human factors. In addition to implementing cybersecurity measures, it is crucial for relevant personnel to be vigilant and recognize signs of a compromised computer system. Indicators to watch out for, include an unresponsive or sluggish system, unexpected password changes or authorized users being locked out, errors in programs or unusual program behaviour, sudden changes in available disk space or memory, emails being returned unexpectedly, difficulties with network connectivity, frequent system crashes, abnormal hard drive or processor activity, and unexpected changes to browser, software, or user settings. These signs should be treated as potential cyber incidents, and designated personnel should be able to comprehend reports from intrusion detection systems (IDS) if they are in use.

Furthermore, these guidelines assume that other key stakeholders involved in the supply chain, such as charterers, classification societies, and service providers, will also adhere to best practices in cybersecurity protection and training. Ship owners and operators are advised to assess the cyber security preparedness of their third-party providers, including marine terminals and stevedores, as part of their sourcing procedures for such services. This ensures that the entire supply chain follows robust cybersecurity practices to minimize potential vulnerabilities and risks.

There are organizations offering cyber security awareness and training programs for the maritime industry. One instance is DNV that offers the DNV Maritime Cyber Security Awareness E-learning program[40] which primarily addresses the human factor in cybersecurity. According to DNV, a significant proportion of attacks (97%) comprise social engineering techniques aimed at deceiving users into opening attachments that contain malicious content. DNV's e-learning course raises awareness about such threats and encourages good cyber hygiene among crews and shore staff. The course is designed for a broad audience and leverages key safety management practices for application to

cybersecurity within the maritime industry. The training can be accessed online and comprises four modules that outline the role of each individual in preventing cybersecurity breaches and mitigating impact in the event of a successful cyber-attack. The modules cover a range of topics including common threats and traps, good practices towards cybersecurity, and security countermeasures. The program emphasizes how changing behaviour can contribute significantly to cybersecurity. DNV's e-learning course not only addresses the IMO Resolution MSC.428(98)[41] but also promotes responsible behaviour by shore-based and vessel personnel regarding cybersecurity threats, which have been on the rise in maritime industries.

Another example is Lloyd's Register (LR) that offers a one-day course on Maritime Cyber Security Awareness[42]. The LR course covers the principles and key practical aspects of effective maritime cybersecurity risk management. The training includes presentations, group discussions, case studies, and exercises on topics such as regulatory requirements, potential cybersecurity threats, risk assessment, risk mitigation strategies, third-party specialist support, and the implementation of an effective cybersecurity risk management plan. The course is intended for anyone whose role is affected by maritime cybersecurity. It aims to equip participants with the ability to contribute more effectively to the management of cybersecurity risks. The aim of this course is to allow participants to be able to interpret the current regulatory landscape, consider a variety of potential cybersecurity threats, assess associated risks, recommend mitigating measures, and contribute towards the continual improvement of their organization's cybersecurity risk management performance.

While DNV offers an e-learning format that allows for flexible learning, Lloyd's Register provides a concentrated one-day course. Both training programs adhere to international regulations and standards, underscoring their commitment to promote responsible behaviour in maritime cybersecurity.

Computer access for visitors

In order to maintain a secure environment onboard maritime vessels, it is essential to implement strict access control measures for visitors, including authorities, technicians, agents, port and terminal officials, and owner representatives. These individuals should have restricted computer access privileges while onboard to prevent unauthorized entry into sensitive or critical computer systems. It is crucial to strictly prohibit unauthorized access to these systems. In cases where network access is necessary and authorized for visitors, it should be closely supervised and limited in terms of user privileges. Access to specific networks for maintenance purposes should be approved and coordinated following the appropriate procedures established by the company or ship operator. To ensure further protection against unauthorized access, visitors requiring computer and printer access should be provided with an independent computer that is isolated from all controlled networks. This isolation prevents any potential risks associated with accessing sensitive networks. Additionally, to mitigate the risks of unauthorized access through physically accessible computers and network ports, the use of removable media blockers should be implemented on all other devices. These blockers act as a safeguard by preventing the insertion of unauthorized removable media, thereby reducing the potential for security breaches.

Crew’s personal devices

To ensure the secure use of IT devices for personal and leisure purposes aboard maritime vessels, it is essential to establish comprehensive procedures and guidelines. These procedures should encompass instructions and protocols for crew members on utilizing the ship's communication networks for personal activities like Skype, emails, gaming, and video streaming. The objective is to strike a balance between allowing crew members to enjoy these amenities while safeguarding the integrity and functionality of critical IT and OT systems. By providing clear instructions, crew members can navigate personal internet usage without inadvertently endangering the vessel's vital systems. This proactive approach acknowledges the importance of addressing potential cybersecurity risks stemming from personal device usage while maintaining an environment that respects the well-being and recreational needs of the crew.

Upgrades and software maintenance

In order to maintain a robust cybersecurity posture, it is crucial for companies to carefully evaluate the use of hardware or software that is no longer supported by its manufacturer or developer. The reason is that such systems may not receive updates to address potential vulnerabilities, leaving them susceptible to exploitation. As part of the cyber risk assessment process, it is important to consider the implications of using unsupported hardware or software. Keeping relevant hardware and software installations up to date is essential for maintaining an adequate level of security on board maritime vessels. Establishing procedures for timely software updates becomes necessary, considering factors such as the ship type, internet connectivity speed, and sea time. This includes not only computer operating systems but also routers, switches, firewalls, and various OT devices that may require regular firmware updates. The procedural requirements should encompass the management of these updates.

Ensuring effective software maintenance relies on the identification, planning, and execution of measures throughout the entire software lifecycle. To assist in maintaining safe and secure software, an industry standard[43] has been developed. This standard outlines specific requirements for all stakeholders involved in software maintenance of shipboard equipment and associated integrated systems. It encompasses on-board, on-shore, and remote software maintenance, aiming to establish consistent practices across the industry. As reported in the industry standard on software maintenance of shipboard equipment by BIMCO and CIRM (Comité International Radio-Maritime), the software maintenance process flow is the following:

1. Event Initiation: This is the first process in the flow and it involves the initiation of the software maintenance event. This could be for preventative or corrective maintenance, regulatory compliance, or improvement of performance.
2. Planning: The event should be properly planned before execution to optimize software maintenance arrangements and ensure the best possible outcome. This process involves close communication between all relevant roles and includes considerations such as who will be involved, what will be done, when and where it will take place, and the maintenance of an onboard software log.
3. Execution: This is the process when the software maintenance is actually carried out on. It is essential that this process is conducted in accordance with the planning

process. During execution, it is imperative to protect the equipment against cybersecurity threats. This involves execution and control measures, as well as cybersecurity precautions.

4. After-service: Following the completion of the execution process, communication between the relevant roles continues in order to monitor the success of the event and provide information that can be used to increase the effectiveness of future planning processes and the success of future events. This includes service reports, onboard software logs, evaluation, and feedback.

Anti-virus and anti-malware tool management

To maintain robust cybersecurity measures in the maritime industry, it is crucial to prioritize the regular updating and management of scanning software tools used for detecting and addressing malware. Malware refers to any type of malicious software[44] that is designed to harm computer systems or steal information. Malware can be introduced into a ship's systems through various means, such as phishing emails, infected USB drives, or software downloads. Once installed, malware can disrupt operations, steal data, or even allow remote access to ship systems.

Establishing procedural requirements becomes essential to ensure that these updates are promptly distributed to ships and that all relevant computers on board are kept up to date. By implementing a systematic approach to software updates, maritime stakeholders can enhance their ability to identify and mitigate potential cyber threats effectively. Malware detection and prevention techniques are essential components of any robust cybersecurity strategy (Cheerala & Kaur, 2021)[45] and antivirus software comes in various types, each designed to combat specific threats and vulnerabilities.

- Signature-based detection is the oldest and most common method of malware detection, which involves comparing the code of a suspicious file with a database of known malware signatures. However, this method has some limitations, such as being unable to detect new or unknown malware, being vulnerable to obfuscation techniques, and requiring frequent updates of the signature database.
- Heuristic-based detection is a method that analyses the characteristics and behaviour of a file rather than its code. This method can detect new or unknown malware that has not been seen before, but it also has some drawbacks, such as generating false positives, being resource-intensive, and being bypassed by polymorphic or metamorphic malware.
- Behaviour-based detection is a method that monitors the actions of a file during its execution and compares them with a set of predefined rules or policies. This method can detect malware that tries to evade static analysis or hide its malicious intent, but it also has some challenges, such as being dependent on the quality and accuracy of the rules or policies, being susceptible to false negatives, and being affected by user interaction.
- Cloud-based detection is a method that leverages the power and resources of cloud computing to perform malware analysis. This method can improve the scalability and efficiency of malware detection, but it also has some issues, such as requiring internet connectivity and bandwidth, raising privacy and security

concerns, and being dependent on the reliability and availability of the cloud service provider.

- Machine learning-based detection as a method that uses artificial intelligence and data mining techniques to learn from large datasets of malware samples and classify them into malicious or benign. This method can overcome some of the limitations of traditional methods and adapt to new and evolving threats, but it also has some challenges, such as requiring high-quality and representative data, being vulnerable to adversarial attacks or noise injection, and lacking explainability or transparency.

Additionally, many of the antivirus solutions available provide sandboxing. This is a technique that isolates a file in a virtual environment and observes its behaviour without affecting the host system. This technique can enhance the security and performance of malware detection, but it also has some limitations, such as being detected and avoided by some malware, being time-consuming and costly, and being dependent on the configuration and compatibility of the virtual environment.

There are several commercially available anti-virus and anti-malware solutions for the maritime environment. Dualog Endpoint[46] is one such solution designed specifically for the maritime industry. This solution is powered by the ESET Endpoint and offers advanced threat detection and response. It provides multi-layered security and controls for vessels' cybersecurity and is designed to counter an ever-growing variety of threats that can target ships. It provides fleet-wide antivirus and malware protection and is designed to protect crew, assets, and operations from attacks. The product also offers advanced malware protection. Dualog Endpoint is also designed to be simple to deploy and easy to administer, with a small footprint that allows it to run smoothly on older systems with limited resources. Dualog Endpoint also offers over-the-air deployment and updates with minimal data usage, ensuring the system stays up-to-date even in the challenging maritime environment.

Another instance is GTMaritime's GTSentinel[47] that represents a complete antivirus solution specifically designed to address the unique cybersecurity challenges within the maritime industry. Unlike traditional antivirus software, GTSentinel provides end-point protection that minimizes impact on communication networks and offers features tailored to maritime needs. More specifically, the platform employs compressed updates distributed throughout the network to reduce data usage and permits flexible update schedules tailored to a vessel's connectivity and budget. Furthermore, GTSentinel offers a centralized dashboard for remote management and control of updates, ensuring optimal security oversight across a vessel's network. Notably, the solution includes robust offline protection capabilities, defending endpoints from various attacks, including known vulnerabilities, exploitable applications, and botnets, and utilizes machine learning for deep network content inspection, all of which maintain protection without internet connectivity.

Secure Remote access

To ensure the utmost security of onboard IT and OT systems, it is important to establish well-defined policies and procedures that govern remote access. These guidelines should leave no room for ambiguity, clearly specifying who is authorized to access the systems, when they can do so, and the specific areas or functionalities they are permitted to

access. To enhance accountability and facilitate effective incident response, it is essential to diligently record every instance of remote access. By maintaining a comprehensive log, any disruptions or anomalies in the IT or OT systems can be reviewed and investigated thoroughly. This documentation serves as a valuable resource for analysing potential security breaches or incidents. Furthermore, it is imperative to identify and define the systems that necessitate remote access, subjecting them to constant monitoring and periodic reviews. This proactive approach helps identify and address any vulnerabilities or areas that require strengthening, ensuring the continuous security and integrity of the ship's IT and OT systems.

Secure Use of administrator privileges

Ensuring secure access to information is a critical aspect of maritime cybersecurity. It is imperative to restrict access to relevant authorized personnel only. Administrator privileges, which grant full access to system configuration settings and all data, should be carefully managed. Users logging into systems with administrator privileges may inadvertently expose existing vulnerabilities, making them more susceptible to exploitation. Therefore, it is crucial to limit administrator privileges to appropriately trained personnel who require such access for their specific roles, whether onboard or within the company. Any usage of administrator privileges should be strictly confined to functions that necessitate such elevated access. Moreover, user privileges should be promptly revoked when an individual is no longer onboard. It is essential to avoid the practice of passing on user accounts from one user to another using generic usernames. Similarly, onshore personnel who have remote access to ship systems should adhere to the same guidelines when they change roles and no longer require access. This diligent management of user privileges helps mitigate the risk of unauthorized access and potential breaches. In the maritime industry, access to onboard systems is granted to various stakeholders, including suppliers and contractors. While these entities play crucial roles, they also pose inherent risks. Suppliers and contractors often possess intimate knowledge of a ship's operations and may have full access to its systems. Therefore, it becomes necessary to implement robust security measures and closely monitor their activities to prevent any unauthorized actions or potential breaches.

Multi/factor authentication (MFA) and secure passwords

To safeguard sensitive information and protect critical systems from unauthorized access, it is crucial to establish a robust password policy coupled with multi-factor authentication. MFA should be implemented across appropriate levels within the organization to enhance security. To mitigate the risk of password attacks, passwords must be strong, and they can be either generated by users or machines. Password attacks refer to any attempt to obtain or crack passwords[48] to gain access to ship systems. Password attacks can be particularly effective if crew members use weak or easily guessed passwords.

To mitigate the risk of such attacks, several protection measures can be implemented. These include enforcing strong password policies. These policies can enforce password complexity requirements and password expiration policies. Password policies can also prevent users from using common passwords or passwords that have been compromised

in previous data breaches. Additionally, multi-factor authentication can be used to prevent unauthorized access to sensitive information. Multi-factor authentication requires users to provide two or more forms of identification before accessing sensitive information. This can prevent attackers from accessing sensitive information even if they manage to obtain passwords through password attacks. Intrusion detection and prevention systems can also be implemented to detect and prevent password attacks. Educating crew members on safe password practices, such as avoiding sharing passwords and using unique passwords for each account, is also crucial. Finally, implementing strict access controls and limiting user privileges can prevent unauthorized access to critical systems. By implementing these measures, organizations can significantly reduce the likelihood and impact of password attacks. Multi-factor authentication requires users to provide additional verification, such as a fingerprint or security token, in addition to a password. MFA is a way of verifying your identity when you sign into an online account or service, using more than one factor or method. A factor is something that you know (such as a password or a PIN), something that you have (such as a smartphone or a security key), or something that you are (such as a fingerprint or a face scan). By using more than one factor, you make it harder for attackers to access your account, even if they know your password or steal your device.

It is important for company policies to strike a balance, avoiding overly complex passwords that require frequent changes, as this can lead to the unsafe practice of writing them down and keeping them near the computer. Passwords should be complemented with the use of MFA, which combines something you have (such as a token or device), something you know (like a password), and something you are (such as a fingerprint passcode on a phone). By implementing MFA, the risk of password compromise is significantly reduced, as the threat actor would not have access to the physical token or device even if they manage to obtain the password.

SG Smart Tech is a vendor that offers a multifactor vessel authentication service, known as ShipAuth[49], that is designed to enhance the security of maritime applications. This service provides multifactor authentication to validate that an application is accessed on a specific vessel.

The operation of the service is as follows:

- Each vessel registers with the ShipAuth Server by downloading the ShipAuth App on the vessel's computer. In this process, a secret key pair is generated. The private key is stored on the local computer. When registering an application instance, verification checks are conducted to ensure that the registration is taking place from the intended vessel. This is accomplished by using the vessel's IMO number, mail ID, and public IP provided by the VSAT ISP.
- Each application that needs to use the service also registers with the ShipAuth Server.
- Applications can request a Time-based One Time Passcode (TOTP). The TOTP, which changes every 30 seconds, adds an extra layer of security by ensuring the authentication process is dynamic and resistant to replay attacks.
- TOTP generation adheres to the industry-standard RFC 6284 protocol[50].
- The validation process is designed with a high level of security in mind. Secret keys are stored in an encrypted form, data movement is also encrypted, and key validation is carried out in a hardware-rooted secure environment.

The multifactor authentication mechanism offered by the ShipAuth service can provide a robust layer of security, reducing the risk of unauthorized access to vessel systems and applications.

Given that the use of satellite phones is widespread in the maritime sector, an interesting MFA solution is the method for implementing multifactor authentication using optimistic fair exchange (OFE)[51]. It is a protocol that allows two parties to exchange items (such as digital signatures or payments) in a fair way, with the help of a trusted third party (called an arbitrator) who is only involved if there is a dispute. This solution aims to address the security and privacy issues that arise when exchanging sensitive data over networks, such as cyber-attacks, unauthorized access, data loss, and dishonest intermediaries. This solution also introduces a novel concept of signaller verification, which is a way to ensure that the sender and receiver of the data are who they claim to be, using SMS messages and location tracking. This method can provide transparency, accountability, and efficiency for multifactor authentication using OFE. This MFA method uses Triple DES algorithm for encryption and decryption, and public and private keys for signature generation and verification.

Physical and removable media controls

When data is transferred from uncontrolled systems to controlled systems, there is always a risk of introducing malware into the network. One method that attackers can exploit is the use of removable media, such as USB drives, to bypass layers of defence and target systems that are not directly connected to the internet. To mitigate this risk, it is crucial to have a well-defined policy regarding the use of removable media. This policy should emphasize that media devices should not be routinely used to transfer information between uncontrolled and controlled systems. However, there are situations where the use of removable media is unavoidable, especially during software maintenance tasks. In such cases, it is important to have procedures in place to mitigate the risk. These procedures may include checking the removable media for malware or verifying the legitimacy of software using digital signatures and watermarks. Policies and procedures related to the use of removable media should also include a requirement to scan any removable media device on a computer that is not connected to the ship's controlled networks. If scanning the media on board is not possible, such as when a maintenance technician is using a laptop, the scanning can be done prior to boarding. It is recommended that companies notify ports and terminals about this requirement to scan removable media before allowing file uploads to the ship's system. This scanning process should be carried out when transferring files such as cargo files, loading plans, national and customs forms, port authority forms, bunkering and lubrication oil forms, ship's stores and provisions lists, software update files, and engineering maintenance files.

Equipment disposal including data destruction

In order to safeguard commercially sensitive or confidential data, it is crucial for companies to have a well-defined procedure in place for disposing obsolete equipment. Such equipment may still contain valuable data that could pose a risk if it falls into the wrong hands. To ensure the complete destruction of data, companies should employ appropriate measures, such as using degaussing tools in accordance with the

manufacturer's instructions. By employing degaussing, which involves altering or erasing the magnetic field of the storage media, any residual data on the equipment can be effectively rendered unrecoverable. This proactive approach to data destruction not only mitigates the potential risk of data breaches but also helps organizations maintain compliance with data protection regulations and safeguard their sensitive information.

The table provided below presents an overview of vulnerabilities alongside their corresponding protection measures.

Vulnerabilities	Protection Measures
Obsolete and unsupported operating systems	• Upgrades and software maintenance • Secure configuration of hardware and software
Unpatched system software	• Upgrades and software maintenance • Application software security (patch management)
Outdated or missing antivirus software and protection from malware	• Anti-virus and anti-malware tool management
Inadequate security configurations and best practices	• Limitation to and control of network ports, protocols, and services • Secure configuration of network devices such as firewalls, routers, and switches • Multi/factor authentication and secure passwords • Secure use of administrator privileges
Shipboard computer networks lacking boundary protection	• Limitation to and control of network ports, protocols, and services • Configuration of network devices such as firewalls, routers, and switches • Wireless access controls • Secure use of crew’s personal devices • Email and web browser protection
Safety critical equipment or systems always connected with shore side	• Limitation to and control of network ports, protocols, and services • Configuration of network devices such as firewalls, routers, and switches • Physical security • Secure satellite and radio communication • Secure remote access
Inadequate access controls to cyber assets, networks, etc. for third parties	• Multi/factor authentication and secure passwords • Computer access for visitors • Secure remote access

Staff inadequately trained and/or skilled to manage cyber risks	• Training and awareness
Missing, inadequate, or untested contingency plans and procedures	• Training and awareness

Table 5. BIMCO's Vulnerabilities and Protection Measures

4. Noteworthy Real-World Threats, Vulnerabilities, and Protection Measures in IT and OT systems

4.1 Definition and types of IT threats and vulnerabilities

Cyber threats are constantly evolving, and maritime sector is no exception. The increasing use and complexity of IT and OT systems in the maritime industry have created new cybersecurity risks. These threats and vulnerabilities can affect the safe and efficient operation of ships, endangering the lives of crew members and passengers, and causing significant economic and environmental damage. A threat is an event or action that may compromise the confidentiality, integrity, or availability of a system or network. A vulnerability is a weakness in a system that can be exploited by an attacker to gain unauthorized access or cause harm.

Information Technology Threats and Vulnerabilities:

- Ransomware: Ransomware is a type of malware[52] that encrypts data on a computer system and demands a ransom payment to restore access. Ransomware can have a significant impact on ship operations, particularly if critical systems are affected.

- Denial of Service (DoS) attacks: A DoS attack[53] involves overwhelming a system with traffic or requests, causing it to crash or become unresponsive. DoS attacks can be used to disrupt ship systems, including communications, navigation, and control systems.

- Remote Access Trojans (RATs): A RAT is a type of malware that allows remote access to a system[54], providing an attacker with control over the infected system. RATs can be used to steal data, disrupt operations, or even take control of ship systems.

- Unsecured Network Access: Unsecured network access refers to any situation where ship systems are connected to unsecured networks. Unsecured network access can leave ship systems vulnerable to a variety of attacks, including malware infections and unauthorized access.

The maritime industry is exposed to various cyber threats such as ransomware, denial of service, remote access trojans and unsecured network access. Therefore, it is essential to adopt effective protection measures to prevent these cyber threats and maintain the safety and security of the maritime sector.

Ransomware

To mitigate the risk of ransomware attacks, several protective measures can be put in place.

- Data Backup: One of the most effective strategies to thwart the adverse effects of a ransomware attack is the routine backup of vital data. By storing a replica of critical information, organizations can promptly retrieve data in the event of an

encryption attack, thereby undermining the perpetrator's leverage. These backups, however, should be securely stored in a location not accessible to potential attackers, creating an additional layer of security.

- Anti-Virus Software: Employing robust anti-virus software offers a second line of defence against ransomware. Anti-virus software, with its ability to recognize and eradicate ransomware strains, provides a critical safeguard for systems, pre-emptively addressing potential threats before they infiltrate the system.
- Personnel Training: Furthermore, enhancing personnel understanding of secure internet practices is essential to the overall security posture. Education should focus on equipping individuals with the knowledge to avoid suspicious links and abstain from opening unsolicited attachments, both common vectors for ransomware.
- Access Controls: Implementing stringent access controls and limiting user privileges can significantly decrease the risk of unauthorized access to crucial systems. By enforcing a need-to-know policy, the potential for inadvertent or malicious insider-facilitated attacks can be reduced, further hardening defenses against ransomware.
- Software Updates: Lastly, the regular updating of software and operating systems is a critical preventive measure. Regular updates, which often contain patches for known vulnerabilities, prevent ransomware from exploiting system weaknesses and gaining unauthorized access.

According to Zhang and Li (2017)[55],there is a secure system design and implementation of data backup and recovery for important business areas. Backup can be classified into different types, such as full backup, incremental backup, differential backup, mirror backup, and online backup.

For the establishment of a secure backup solution, the following options are available:

- Digital certificate authentication: It is a method that uses public key cryptography to verify the identity and legitimacy of the data source and destination. The system uses a trusted third party to issue and manage digital certificates for the backup and recovery operators and machines.
- Role-based access control: It is a method that assigns different permissions and privileges to different roles of the operators and machines. The system uses a role management module to define and enforce the access policies for the backup and recovery operations.
- Business model-based process control: It is a method that regulates the workflow and sequence of the backup and recovery operations according to the business requirements and scenarios. The system uses a business model management module to design and execute the backup and recovery processes.
- Operation log-based audit: It is a method that records and analyses the activities and events of the backup and recovery operations. The system uses an operation log management module to collect and store the operation logs and provide audit reports.

An enterprise solution that can apply to vessels, is Resilio's Connect[56] "Ship to Shore Data Replication and Application Management" that offers automatic, real-time transfers of data sets from ship to shore at the full available bandwidth regardless of the internet connection, round-trip delay and packet loss. Resilio Connect offers a complete solution

for fast and automatic data transfer from ship to shore and vice versa. The transfer protocol is optimized for high-speed transfers and automatically adapts to use the full bandwidth of Wi-Fi when available. The protocol also robustly handles network outages, automatically resuming any failed transfer until it is fully completed. Moreover, it supports selective downloading of only the files that are needed, enabling simple file sharing and data synchronization over low bandwidth VSAT links. Resilio Connect is designed for multi-homed networks, making optimal use of the multiple networks available on the ship. It can be configured to minimize the usage of satellite links, make more use of cellular, and take full advantage of Wi-Fi connections. According to Resilio, data integrity is guaranteed, even with low-quality connectivity including high packet loss and disconnects. Furthermore, Resilio's Micro Transport Protocol (µTP2) was designed to overcome the deficiencies of TCP/IP over latent and lossy WAN connections, ensuring an optimal sending rate.

Denial of Service

To protect against DoS attacks, several preventative measures can be employed. The first solution is to use firewalls. Firewalls can prevent DoS attacks by blocking traffic from known malicious IP addresses and filtering out traffic that appears to be abnormal. Firewalls can also be configured to limit the amount of traffic that is allowed to reach a system, which can help prevent DoS attacks. The second solution is to IPS that can detect and block DoS attacks by monitoring network traffic and detecting abnormal patterns. IPS can also be configured to block traffic from specific IP addresses and to limit the amount of traffic that is allowed to reach a system. The third solution is to use load balancing. Load balancing involves distributing traffic across multiple servers to prevent any one server from being overwhelmed. Load balancing can help prevent DoS attacks by ensuring that no single server is handling too much traffic. These solutions can detect and block malicious traffic, reducing the impact of a DoS attack. Many vendors offer network security solutions, including Cisco, Fortinet, and Palo Alto Networks.

For example, on Cisco products[57] there are some techniques to prevent the DoS attacks.

These techniques include but are not limited to:

- Storm control can be configured based on three parameters: traffic type, threshold level, and action. Traffic type refers to the type of traffic to be monitored, such as broadcast, multicast, or unknown unicast. Threshold level refers to the percentage of the total available bandwidth that the traffic type can consume before triggering an action. Action refers to the action to be taken when the threshold level is exceeded, such as blocking or dropping the traffic.
- Port security can be configured based on three parameters: maximum addresses, violation mode, and aging. Maximum addresses refer to the maximum number of MAC addresses that can be learned on a switch port. Violation mode refers to the action to be taken when an unauthorized MAC address tries to access a switch port, such as shutting down or restricting the port. Aging refers to the time period after which a MAC address is removed from the switch port if it is inactive.
- DHCP snooping can be configured based on two parameters: trusted ports and rate limit. Trusted ports refer to the switch ports that are connected to authorized DHCP servers and can receive DHCP messages without filtering. Rate limit refers

to the maximum number of DHCP packets per second that a switch port can receive before triggering an action, such as dropping or logging the packets.

- Dynamic ARP inspection can be configured based on two parameters: trusted ports and rate limit. Trusted ports refer to the switch ports that are connected to devices with valid IP-MAC bindings and can send ARP packets without validation. Rate limit refers to the maximum number of ARP packets per second that a switch port can receive before triggering an action, such as dropping or logging the packets.
- IP source guard can be configured based on one parameter: binding type. Binding type refers to the method of obtaining IP-MAC bindings for a switch port, such as static or dynamic. Static binding means manually entering the IP-MAC binding for a switch port. Dynamic binding means automatically learning the IP-MAC binding from DHCP snooping.

Remote Access Trojans

To mitigate these risks, several protective measures can be adopted. Firstly, it is crucial to regularly install and update anti-virus software to detect and remove any RATs present on the system. Secondly, the use of intrusion detection and prevention systems can also aid in identifying and preventing RAT attacks before they cause significant harm. Additionally, educating users about safe internet practices such as avoiding downloading suspicious files or opening emails from unknown sources can prevent them from unintentionally downloading and executing RATs. Additionally, implementing strict access controls and limiting user privileges can reduce the risk of unauthorized access to critical systems. Another solution is to use network segmentation. Network segmentation involves dividing a network into smaller subnetworks to prevent attackers from moving laterally within a network. This can prevent RATs from spreading to other systems on a network. Lastly, endpoint security solutions can detect and block malicious activity on a computer system, reducing the likelihood of a RAT infection.

Unsecured Network Access

To address this issue, several protective measures can be implemented. The first solution is to use authentication and authorization protocols. Authentication and authorization protocols can ensure that only authorized users are allowed to access a network. These protocols can require users to provide a username and password or other forms of identification before granting access to the network. The second solution is to use network segmentation. Network segmentation can divide a network into smaller subnetworks to limit access to sensitive information. This can prevent unauthorized users from accessing sensitive information by restricting their access to specific subnetworks. The third solution is to use network monitoring tools. Network monitoring tools can detect unauthorized access attempts and alert administrators to potential security threats. These tools can also monitor network traffic to detect unusual activity and prevent potential attacks before they occur.

According to Zscaler[58] network segmentation divides a network into smaller, more secure segments, reducing the likelihood of an attacker being able to access sensitive areas of the network.

Traditionally, there have been two basic types of network segmentation:

- Physical segmentation uses discrete firewalls, wiring, switches, and internet connections to separate parts of a network. This is the more expensive, less scalable type.
- Virtual segmentation, also called logical segmentation, typically segments network traffic flows using VLANs, which can be protected by the same firewall.

There are some best practices to follow when implementing network segmentation.

1. Avoid excessive segmentation as it can limit network visibility and increase management complexity, but also avoid insufficient segmentation as it can lead to a broader attack surface and weaker security posture.
2. Regularly conduct audits to ensure vulnerabilities are addressed, permissions are properly managed, and updates are installed. Auditing network segments ensures comprehensive coverage and mitigation of potential risks.
3. Adhere to the principle of least privilege when granting access to users, network administrators, and security teams across network segments. This approach restricts access to only necessary users and is fundamental for zero-trust network access.
4. Limit third-party access to network segments and grant it only when necessary to mitigate potential risks.
5. Automate network segmentation where possible to improve network visibility, reduce mean time to repair (MTTR), and enhance security posture. This allows for efficient identification and classification of new assets and data.

The following table presents an overview of IT vulnerabilities and corresponding protection measures:

	Ransomware	**Denial of Service**	**Remote Access Trojans**	**Unsecured Network Access**
Antivirus	X		X	
Limit User Permissions	X		X	X
Network Monitoring		X		X

Backup	X			
Security Awareness			X	
Email Security	X			
Firewall		X		
IPS/IDS		X	X	X
Encryption				X
EDR			X	
Patch Management	X			

Table 6. IT Vulnerabilities and Protection Measures

4.2 Definition and types of IT & OT threats and vulnerabilities

Operational Technology Threats and Vulnerabilities:

- Lack of Segmentation: Segmentation refers to the practice of dividing a network into smaller, isolated networks[59] to limit the impact of a security breach. In the maritime industry, ship systems may not be properly segmented, making it easier for attackers to gain access to critical systems.

- Lack of Redundancy: Redundancy[60] refers to the practice of having backup systems in place to ensure continued operations in the event of a failure. In the maritime industry, lack of redundancy can leave ship

- Legacy Systems: Legacy systems[61] refer to outdated systems that may not be compatible with newer software or hardware. In the maritime industry, ships may have legacy systems that are difficult to maintain or update, leaving them vulnerable to attacks.

- Supply Chain Attacks: Supply chain attacks[62] refer to any attack that targets a third-party vendor or supplier that provides components or software for ship

systems. Supply chain attacks can be difficult to detect and can result in compromised ship systems.

- Lack of Monitoring: Lack of monitoring refers to situations where ship systems are not properly monitored for security breaches or anomalous activity. This can leave ship systems vulnerable to attack, as attackers may be able to compromise systems without detection.

- Interconnected Systems: Interconnected systems[63] refer to situations where ship systems are connected to each other or to external networks, such as port networks or satellite networks. Interconnected systems can increase the risk of attack, as attackers may be able to move laterally through ship systems or gain access to external networks.

Lack of Segmentation

The lack of network segmentation is a serious cybersecurity challenge for the marine sector. Due to the interconnected nature of the networks and systems on ships, a cyberattack on one system can spread fast to other systems, creating this vulnerability. Several steps must be taken to achieve adequate protection. First, performing a network segmentation evaluation assist in determining the areas that need segmentation and the kind of segmentation required. Second, the primary line of defence against these types of attacks is proper network segmentation. In order to stop the spread of a cyberattack, this procedure entails slicing the ship's network into smaller, isolated pieces. By keeping the systems apart, an attacker who obtains access to one system will be unable to quickly access others. Systems on the ship should be divided into several zones according to their purposes. The ship's network must also be protected by firewalls and Access Control Lists (ACLs), which restrict access to crucial systems and restrict traffic that violates specified security policies.

Cisco's Network Segmentation Solution[64] is an enterprise-level security solution that is designed to provide enhanced network security by segmenting the network infrastructure into multiple secure zones. The solution is based on Cisco TrustSec technology, which is a software-defined networking (SDN) solution that provides end-to-end security across the network. The solution includes a range of features such as authentication, access control, encryption, and policy enforcement, which are designed to help organizations mitigate security risks and prevent unauthorized access to their network infrastructure. One of the key benefits of the Cisco Network Segmentation Solution is that it helps organizations to reduce their attack surface by limiting access to sensitive resources only to authorized users. The solution also provides granular visibility and control over network traffic, which helps organizations to detect and respond to security threats more quickly. Additionally, the solution is highly scalable and can be easily deployed across complex network architectures, making it an ideal solution for enterprises with multiple locations and complex security requirements.

Lack of Redundancy

The absence of redundancy in ship systems makes maritime cybersecurity vulnerable. This lack of redundancy raises the possibility of a system failure, which might have serious consequences including the loss of life and assets. Protective measures must be put in place to address this risk. In order to identify important systems that need redundancy and determine the amount of redundancy necessary, it is first necessary to

conduct a redundancy assessment. The addition of backup systems in the form of additional hardware, software, or data storage is one example of an appropriate redundancy measure that should be established. Redundancy measures involve putting in place backup or duplicate systems that can take over in the event of a system breakdown. In order to confirm that backup systems are functional and dependable in the event of a catastrophe, regular system checks should also be carried out. Organizations in the maritime industry should put in place failover mechanisms that, in the case of a breakdown, switch over to backup systems. These protection measures are critical in safeguarding against system failure and mitigating the potential impacts of maritime cybersecurity breaches.

Legacy Systems

Due to the obsolete legacy systems that are lacking the most recent security updates and patches and are therefore extremely vulnerable to attacks, the maritime sector has been dealing with a significant cybersecurity risk. Consequently, in order to reduce the possible dangers, marine operators need to take appropriate protective measures. Replacing the obsolete legacy systems with newer, more secure ones is one of the suggested solutions. This strategy appears to be successful since newer systems have greater security measures that can counteract current cyberthreats. Regular vulnerability assessments are essential to find and address any vulnerabilities, in addition to replacing old systems. Alternatively, ships could implement security measures such as firewalls, intrusion detection systems, and access control lists to protect legacy systems. System patching and upgrading should be done on a regular basis to make sure that vulnerabilities are found and fixed right away. The risks associated with legacy systems can be reduced and maritime operators should make sure that their ships are sufficiently protected against cyberattacks by adhering to these protection measures.

Supply Chain Attacks

The rising number of supply chain attacks has recently been a significant issue. In order to acquire unauthorized access to the ship's network and systems, cybercriminals now target the supply chain of ships, which includes vendors and suppliers. Implementing robust vendor management processes and ensuring that all suppliers adhere to cybersecurity requirements are two aspects of supply chain security solutions. Conducting regular supply chain security assessments can help identify potential vulnerabilities in the supply chain that may lead to cyber-attacks. Maritime organizations should conduct due diligence on suppliers to ensure that they have appropriate security measures in place. Second, implementing supply chain security measures, such as regular supplier vetting, establishing contractual obligations for suppliers to maintain security standards, and conducting regular supplier security audits can help bolster the overall security of the supply chain. Furthermore, performing periodical supply chain security audits could help in making sure that these security measures continue to be relevant and efficient over time.

Lack of Monitoring

The absence of proper monitoring poses a challenge to detecting and responding to cyber threats. To address this challenge, certain protective measures can be implemented. Continuous monitoring is a method that involves continuously monitoring a ship's network and systems to identify potential cyber-attacks and respond to them swiftly. Another useful tool is security information and event management (SIEM), which collects and

analyses security events from a ship's network and systems, aiding in the identification of potential cyber-attacks and enabling quick response. These systems should be regularly monitored for potential security breaches, and any suspicious activity should be investigated promptly. In addition, regular security assessments can be conducted to identify areas that require additional monitoring and improve existing monitoring capabilities. Continuous monitoring measures involve implementing automated monitoring tools that can detect and alert personnel of any suspicious activity on the network or system.

BRIDGE[65] is a transformative solution that simplifies the consumption of Cyber Threat Intelligence (CTI) for SOC teams, Sec/IT Analysts, CSIRTs, and more. Its three core modules -parser, translator, and data pool- ensure interoperability, data integrity, and efficient intelligence extraction. CTI reports, formatted in STIX 2.1, are securely stored in a blockchain-based Data Pool, while the Translator provides SOC teams with Sigma files for standardized detection rules. These Sigma files empower SOC teams to detect and respond to indicators within CTI reports using their SIEM tools, enhancing cybersecurity capabilities organization-wide.

CyberOwl, a company specializing in maritime cybersecurity, provides a solution for monitoring and analytics of operational assets[66]. Its product suite is designed to offer visibility, security, and compliance. The core of its solution lies in Medulla, a cybersecurity monitoring and analytics system considered one of the most advanced in the maritime sector. Medulla presents unrivalled visibility, offering meaningful visualizations of the cyber risks of onboard systems across the entire fleet in real-time. This system also provides actionable intelligence by escalating early warnings of cyber-attacks on onboard IT, IoT, and OT systems and prioritizes these warnings for remediation based on asset criticality. Medulla is designed to address and overcome the technical and operational challenges of maritime and remote environments. It offers an asset-centric approach, allowing users to quickly visualize the specific asset on the specific vessel where there is an escalating cyber risk and assess its criticality. This system integrates effortlessly with existing SIEM tools and ensures continuous monitoring and analytics despite communication dropouts and analyses multiple data sources to provide in-depth visibility, including protocols, network traffic, host logs, and operational logs. Moreover, Medulla is designed for simple, intuitive installation by crew, using "plug and play" technology to avoid the need for vessel visits.

Interconnected Systems

Interconnected systems in maritime, pose a significant vulnerability as a cyber-attack on one system can easily spread to other interconnected systems. It is essential to take proactive measures to mitigate this risk. One recommended measure is conducting system interconnectivity assessments to identify interconnected systems and determine their level of risk. Another critical protection measure is implementing proper network segmentation, which helps to prevent cyber-attacks from spreading to interconnected systems. Furthermore, implementing intrusion detection and prevention systems (IDPS) is a solution that can monitor a ship's network for potential cyber-attacks and take action to prevent them from spreading.

Intrusion detection systems utilize various methods to identify intrusions such as:

- Signature-based detection involves checking for specific behaviour or patterns, such as malicious signatures or byte sequences, to identify attacks. This approach

is effective for known cyberthreats but may struggle with new attacks where a pattern cannot be traced.
- Reputation-based detection involves assessing the reputation scores of cyberattacks, allowing traffic with good scores to pass while alerting the user to take action for those with poor scores.
- Anomaly-based detection monitors network activities to detect computer and network intrusions and violations, utilizing machine learning to build a trustworthy activity model and compare it against new behaviors. This approach can detect both known and unknown attacks.

In-depth scrutiny of network traffic is performed by intrusion prevention systems through the utilization of one or more detection methods, such as:

- Signature-based detection, where the IPS keeps track of network traffic to detect attacks and matches it with predefined attack patterns
- Stateful protocol analysis detection, which involves identifying anomalies in a protocol state by comparing current events with accepted activities that are predefined
- Anomaly-based detection, whereby the IPS monitors data packets by comparing them against a normal behaviour to detect new threats, albeit with the possibility of producing false positives.

One IDPS solution is Snort[67]. It is an open-source, rule-based IDPS that analyses network traffic in real-time to detect and prevent a wide range of threats, such as malware, viruses, and network attacks. Snort uses a combination of signature-based and anomaly-based detection techniques to identify and respond to security threats, making it a highly effective tool for network security. The sniffer component captures network packets and sends them to the detection engine, which analyses the packets based on predefined rules and signatures to identify any malicious behaviour. Once a threat is detected, Snort can generate alerts and take actions to prevent the threat from causing further harm. Snort provides a wide range of features and capabilities, including real-time traffic analysis, packet logging, alerting and reporting, and customizable rule sets. It also supports a variety of deployment options, including standalone systems, network appliances, and virtualized environments.

The following table presents an overview of OT vulnerabilities and corresponding protection measures:

	Lack of Segmentation	**Lack of Redundancy**	**Legacy Systems**	**Supply Chain Attacks**	**Lack of Monitoring**	**Interconnected Systems**
Patch Management			X			
Vulnerability Assessment			X			

Network Segmentation	X					X
Firewall	X					
Limit User Permissions	X					
Backup		X				
IPS/IDS						X
Due Diligence				X		
Network Monitoring					X	

Table 7. OT Vulnerabilities and Protection Measures

5. Best Practices

This chapter encapsulates a summary of strategies and procedures that have been derived through extensive dialogues with shipping companies and maritime organizations. These entities, operating at the vanguard of the maritime sector, have integrated these practices into their operational framework to bolster maritime cybersecurity. The practices mentioned in this chapter are not merely theoretical propositions, but rather, they are the embodiment of the collective expertise and experiential knowledge of these organizations in their pursuit to fortify their cyber environment.

The design of a ship's network architecture is critical to ensure the reliable and secure communication between different systems. The architecture must take into account several essential aspects to guarantee the network's integrity and confidentiality. One of these aspects is segmentation, which involves dividing the network into different parts to prevent a security breach from affecting the entire network. This approach guarantees that any security breach in one section of the network does not compromise the other sections. Additionally, redundancy is a crucial aspect of the ship's network architecture, as it ensures continuous operation in the event of component failure. Redundant systems guarantee that the network remains operational even if one or more components fail. Access control is another crucial element of the ship's network architecture, which involves implementing both physical and logical access control measures to ensure that only authorized personnel have access to the network. Lastly, continuous monitoring is necessary to detect and prevent security breaches. This monitoring includes the use of IDS and SIEM tools. Therefore, the design of a ship's network architecture must consider these critical aspects to guarantee the network's reliability and security.

To adhere to cybersecurity best practices, GTM[68], a cybersecurity investment tool has been developed, serving as a valuable resource for a wide spectrum of cybersecurity professionals, from CISOs to security researchers. GTM leverages attack graphs and game theory to proactively predict attack scenarios and strategically allocate cybersecurity budgets, ensuring optimal risk mitigation.

5.1 Onshore best practices

User Access

To ensure the appropriate allocation of access rights and permissions, it is necessary to assign each user permissions based on their expected job duties. For a department to request access to the systems, approval from the supervisor must be obtained, and the request should be submitted accordingly. It is crucial that user accounts outside of the group role are not granted additional permissions, and that group roles are maintained in accordance with business positions. If a user acquires a different role, their old role must be revoked. To avoid granting unnecessary privileges, it is advisable that System and Network Administrators refrain from using user accounts with privileged access for day-to-day tasks and instead use admin accounts only when additional privileges are needed. Access to admin level permissions should only be granted to individuals whose roles require them. Lastly, it is recommended that a review of user access privileges is conducted at least annually to ensure that access rights are still appropriate for each user's job function.

Supplier Access

When the company allows external vendors to access particular systems to offer remote assistance for its business applications, the level of access granted to these vendors is pre-defined, restricted and monitored. This is determined by the requirements of the support they are providing. If any of the suppliers' employees leave their position, the supplier must notify the Cyber Security Officer in a timely manner, to avoid any unauthorized access to the network. These policies regarding access control, when implemented, ensure that external parties are only allowed limited and monitored access to the company's network. This strategy serves to mitigate the risk of unauthorized access and potential security breaches.

Protection from malware

In order to reduce the risk of virus infections, it is essential to implement a range of protection measures. These measures encompass a thorough assessment of malware protection software before its procurement. Installing anti-virus software across all servers and endpoint devices, is crucial to prevent virus attacks. Firewall settings must be configured to detect and prevent known and unknown threats, including viruses, bots, phishing attacks, and malicious applications. Automatic updating of anti-virus software should also be enabled. In addition, configuring settings on individual devices, such as disabling USB auto-run, configuring browsers to disable pop-ups, and disabling macro commands can minimize the risk of malicious code infections. Furthermore, corporate mobile phones and laptops should be registered on a management console to ensure encryption and compliance with security standards. Access to software installation on corporate PCs should be restricted to authorized personnel only. The IT department must approve all software installations prior to installation, and only authorized USB connections should be allowed on company PCs. Finally, it is recommended to perform centralized operating system patching to enhance security and prevent unauthorized system intrusions.

Logging and monitoring

The safety and security of ships' ICT systems rely heavily on the monitoring and detection of threats. Various systems, including firewalls, intrusion detection and prevention systems, and gateways to other networks are subject to monitoring. System and Network administrators have to be automatically alerted when potential threats are detected, which encompass unauthorized access attempts, system alerts or failures, and system capacity alerts when reaching a defined threshold. It is critical to analyse and document incidents immediately upon receiving alerts. The monitoring system should be optimized, and the underlying issue addressed if an excessive number of alerts are generated. Consequently, maintaining the organization's security relies significantly on the effective monitoring and management of threats to the vessels' ICT systems.

Password Security

The preservation of the integrity and security of maritime ICT systems is significantly reliant on the assurance of strong password security. Since passwords are often the initial line of defence against unauthorized access, they may be compromised through various means, including social engineering and password attacks. The maritime industry has thus to establish specific password security requirements to mitigate these threats. One of the essential factors in ensuring robust password security is password creation. Maritime personnel should create intricate passwords that are hard to guess or crack,

which should not comprise identifiable data such as birth dates, names, or social security numbers. The password should contain a combination of symbols, numbers, upper and lower case letters, and the length should meet a minimum standard, typically ranging between 8-12 characters. Password change is another vital aspect of password security. The maritime industry should make it obligatory to change passwords periodically, requiring personnel to update their passwords after a set time, usually ranging from 30 to 90 days. The password change interval may vary based on the sensitivity of the data being protected. Regular password changes minimize the risk of password-based attacks and enhance password security.

Network Security Design

The design of a network security system must incorporate various fundamental security principles to ensure its effectiveness. These principles encompass several key aspects, such as identifying potential network threats, assessing trust levels between different systems and networks requiring connection, determining the required level of network availability, and considering the network's geographical distance and future expansion. In addition, deploying a Firewall and an IDS/IPS is highly recommended for centralized network administration and monitoring. VLANs may also be employed when needed to enhance network security. Additionally, robust encryption techniques have to be followed in order to safeguard the confidentiality of transmitted data.

Patch Management

Patch management is a critical component of ensuring the security and stability of a company's network. To maintain an effective patch management system, it is important to follow several best practices. Firstly, all software and operating systems used within the company should be kept up to date with the latest security patches and updates. Secondly, all updates should be tested in a testing/staging environment before being applied to production systems to ensure compatibility and avoid any unforeseen issues. Thirdly, a schedule should be established for regular patching, with priority given to high-risk and critical vulnerabilities. Moreover, patching should be monitored and tracked to ensure that all systems are up to date and any gaps in security are identified and addressed promptly. Patch management policies and procedures should be documented and communicated to all relevant stakeholders to ensure that everyone is aware of the importance of patching and the steps involved in the process. Finally, regular reviews of the patch management system should be conducted to identify any areas for improvements and to ensure that the system remains effective in protecting the company's network from potential cybersecurity threats.

Vulnerability Assessment

Vulnerability assessment is a critical process that helps to identify potential security risks within a company's network infrastructure. To maintain an effective vulnerability assessment program, it is important to follow several best practices. Firstly, a comprehensive inventory of all hardware, software, and applications used within the company should be established. Secondly, all systems and applications should be regularly scanned for vulnerabilities to identify any gaps in security that could be exploited by attackers. Furthermore, the results of vulnerability scans should be analysed to prioritize vulnerabilities based on risk and impact. Additionally, a remediation plan should be established to address identified vulnerabilities. Finally, a schedule for regular vulnerability scanning and remediation should be established, with periodic reviews to ensure that the program remains effective in identifying and addressing security risks.

5.2 Onboard best practices

Crew Access Rights

The allocation of crew access rights and permissions is a crucial aspect of managing system security and ensuring that tasks are performed efficiently. It is imperative to assign access rights and permissions that align with the crew's expected tasks. The allocation of additional permissions beyond the necessary ones must be avoided to maintain a secure and controlled system. The administration of crew account permissions should be restricted to authorized personnel only, such as system administrators, who are responsible for viewing and updating the permissions of crew accounts.

Privileged Access Rights

The effective management of privileged access rights is an essential aspect of system and network administration. It is crucial to identify the specific privileged access rights associated with administrator-level accounts for each system or network and establish strict controls over such access. To minimize the risk of unauthorized access and potential misuse of admin level permissions, access should only be allocated to individuals whose roles explicitly require it, and who have received adequate training to fully comprehend the consequences of their actions. These measures ensure that privileged access rights are utilized in a responsible and secure manner and minimize the risk of security breaches and data loss.

Network Infrastructure

The network infrastructure should consist of two distinct networks: the Operational Network and the Crew Network. The Operational Network is solely utilized for the interconnection and operation of the IT and OT systems present onboard. In contrast, the Crew Network is a segmented network that is primarily designed for Internet access, specifically for the use of crew members and visitors. The segregation of the two networks ensures that the critical business functions are secured and isolated from the potential vulnerabilities posed by external connections, while also providing a separate platform for crew members to access the Internet without interfering with the essential business operations.

Network Protection

Network protection against unauthorized access and malicious activities is not confined to any single sector but extends ubiquitously across all industries, including the maritime sector. To mitigate such security risks, various measures can be taken to safeguard the network infrastructure. One such measure is the implementation of firewall protection, which allows only authorized network traffic to pass through. In addition, network equipment can be installed in secure racks on the bridge of the vessel, limiting physical access to only authorized personnel. Another security measure is disabling unused switch and router ports to prevent unauthorized access.

Restricted Access to USB ports

The unauthorized use of removable media devices on Vessel's IT and OT equipment should be strictly prohibited. In order to enforce this policy, all USB ports on IT equipment should be blocked to non-authorized removable media devices. Additionally, USB ports

on OT systems should be blocked and only unblocked for business or troubleshooting purposes using a special key. The distribution of USB unblocking keys to successors during changeover must be documented. Transfer of information to a vessel's PCs from visitors/guests should be conducted via a dedicated visitor/guest PC using an authorized media device, and visitor/guests PCs are not connected to the vessel’s network. Finally, it should be strictly prohibited to charge personal phones and devices in vessel's equipment with USB ports. These measures are designed to protect the integrity and security of ship’s IT and OT systems.

6. Conclusions

The complexity of modern maritime vessels makes them more vulnerable to cyber-attacks. Therefore, it is essential to implement robust cybersecurity measures to mitigate these risks. The following are some key steps that can be taken to improve cybersecurity in maritime:

- Conduct Regular Risk Assessments: Conducting regular risk assessments can help identify potential cybersecurity threats and vulnerabilities, allowing for the implementation of appropriate mitigation measures.
- Implement Multi-Layered Security: Implementing multi-layered security measures, including firewalls, antivirus software, and network segmentation, can help prevent cyber-attacks.
- Train Crew Members: Crew members should be trained on basic cybersecurity practices, such as identifying phishing emails and avoiding public Wi-Fi networks.
- Conduct Regular System Audits: Regular audits of vessel systems can help identify any vulnerabilities or potential breaches, allowing for appropriate mitigation measures.
- Implement Secure Network Architecture: Implementing secure network architecture, including network segmentation and access control, can help prevent unauthorized access to critical systems.

Despite these best practices and protection measures, it's important to recognize that the maritime industry is not completely secure. Several challenges and factors contribute to this lack of complete security:

- Evolving Threat Landscape: The maritime sector faces a dynamic and ever-evolving cyber threat landscape. Adversaries continually develop new tactics, and techniques, making it difficult to predict and prevent cyber-attacks effectively.
- Legacy Systems: Many vessels still operate with legacy systems, which were not originally designed with cybersecurity in mind. Retrofitting these older systems with modern security measures can be a resource-intensive and complex process.
- Interconnected Systems: Modern vessels depend on a complex network of integrated systems and networks, which expands the attack surface and potential vulnerabilities.
- Regulatory Challenges: The regulatory landscape for maritime cybersecurity is still evolving. Compliance and enforcement can vary, and keeping up with the latest regulations poses challenges for maritime industry stakeholders.
- Supply Chain Risks: The maritime sector's global supply chain introduces additional cybersecurity risks, such as compromised components or software vulnerabilities in third-party systems.
- Human Element: Human error remains a significant vulnerability. Despite training and awareness initiatives, crew members can inadvertently introduce security risks, such as falling for social engineering attacks. Ensuring comprehensive cybersecurity competence among all crew members is an ongoing challenge.

In summary, a holistic approach to maritime cybersecurity is required. One that combines industry-tested strategies, technical and procedural protection measures , and continuous training and awareness initiatives. It is through this comprehensive approach that the

maritime sector can effectively navigate the complex landscape of cybersecurity threats and ensure the safety and security of its operations. The maritime sector's increasing reliance on technology and automation has given rise to new cybersecurity risks that might have a significant impact on the sector. The marine industry's examples of cyberattacks show the potential financial, reputational, and safety implications linked to these threats. To minimize these risks and guarantee the ongoing safe and effective operation of international trade and transportation, there is a clear need for increased research and attention to be paid to cybersecurity in the marine industry.

References

1) National Maritime Cybersecurity Plan. (n.d.). Retrieved from https://www.maritime-cybersecurity.com/National_Maritime_Cybersecurity_Plan.html
2) Digital Guardian. (2020, August 7). The Cost of a Malware Infection: Maersk's $300 Million Loss. Retrieved from https://www.digitalguardian.com/blog/cost-malware-infection-maersk-300-million
3) BBC News. (2018, September 27). Maersk cyber attack: Shipping giant admits 'vulnerabilities'. Retrieved from https://www.bbc.com/news/technology-45677511
4) Comprehensive Guide to Maritime Security [Ebook]. (2020). Retrieved from https://www.missionsecure.com/resources/comprehensive-guide-to-maritime-security-ebook
5) Frank Akpan, Gueltoum Bendiab, Stavros Shiaeles, Stavros Karamperidis, Michalis Michaloliakos. (2022, March 7). Retrieved from https://www.mdpi.com/2673-8732/2/1/9
6) SOLAS V on Safety of Navigation [PDF]. (2002). Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/343175/solas_v_on_safety_of_navigation.pdf
7) Petihakis, G., Kiritsis, D., Farao, A., Bountakas, P., Panou, A., & Xenakis, C. (2023, August). A Bring Your Own Device security awareness survey among professionals. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-10).
8) Maritime Cyber Security. (n.d.). Retrieved from https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html
9) Stoyno Stoynov, Borislav Nikolov. (2021). Retrieved from https://doi.org/10.53656/ped21-7s.16appr
10) Maritime Cyber Security. (2021, March 5). Retrieved from https://www.packetlabs.net/posts/maritime-cyber-security/
11) Maritime Cyber Priority 2023. (2023). Retrieved from https://www.dnv.com/cybersecurity/download/maritime-cyber-priority-2023-receipt.html
12) Comprehensive Guide to Maritime Security [Ebook]. (2020). Retrieved from https://www.missionsecure.com/resources/comprehensive-guide-to-maritime-security-ebook
13) The Guidelines on Cyber Security Onboard Ships. (2020). Retrieved from https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships
14) Document of Compliance (DOC). (n.d.). Retrieved from https://www.lawinsider.com/dictionary/document-of-compliance-doc
15) Victor Bolbot, Ketki Kulkarni, Päivi Brunou, Osiris Valdez Banda, Mashrura Musharraf. (2022, October 30). Retrieved from https://www.sciencedirect.com/science/article/pii/S1874548222000555
16) Leonidou, P., Salamanos, N., Farao, A., Aspri, M., & Sirivianos, M. (2023, August). A Qualitative Analysis of Illicit Arms Trafficking on Darknet Marketplaces. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-9).
17) Hunt & Hacket, Cybersecurity for the Maritime sector. (n.d). Retrieved from https://www.huntandhackett.com/sectors/maritime
18) Panda, S., Farao, A., Panaousis, E., & Xenakis, C. (2021). Cyber-Insurance: Past, Present and Future. In Encyclopedia of Cryptography, Security and Privacy (pp. 1-4). Berlin, Heidelberg: Springer Berlin Heidelberg.
19) Farao, A., Paparis, G., Panda, S., Panaousis, E., Zarras, A., & Xenakis, C. (2023). INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain. International Journal of Information Security, 1-25
20) Farao, Aristeidis, et al. "SECONDO: A platform for cybersecurity investments and cyber insurance decisions." Trust, Privacy and Security in Digital Business: 17th International Conference, TrustBus 2020, Bratislava, Slovakia, September 14–17, 2020, Proceedings 17. Springer International Publishing, 2020.

21) Charalambous, M., Farao, A., Kalantzantonakis, G., Kanakakis, P., Salamanos, N., Kotsifakos, E., & Froudakis, E. (2022, August). Analyzing Coverages of Cyber Insurance Policies Using Ontology. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-7).
22) EVO Series. (n.d.). Retrieved from https://marpoint.gr/evo-series/
23) Firewall Configuration. (n.d.). Retrieved from https://marel.gr/firewall-configuration/
24) Partners. (n.d.). Retrieved from https://marel.gr/partners/
25) Physical Security. (n.d.). Retrieved from https://www.gartner.com/en/information-technology/glossary/physical-security
26) Ahonen, S. (2020). Cyber security of highly automated connected machines (Master's thesis). Retrieved from https://www.theseus.fi/bitstream/handle/10024/497138/Cyber_security_of_highly_automated_connected_machines_Ahonen_Sami_YTC19S1.pdf
27) Thales. (n.d.). Hardware Security Modules. Retrieved from https://cpl.thalesgroup.com/encryption/hardware-security-modules
28) Trusted Computing Group. (n.d.). Trusted Platform Module (TPM) Summary. Retrieved from https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/
29) Cryptographic Standards and Guidelines. (2016, December 29). Retrieved from https://csrc.nist.gov/Projects/cryptographic-standards-and-guidelines
30) Maritime Connect. (n.d.). Retrieved from https://www.orange-business.com/en/solutions/internet-networks/maritime-connect
31) Maritime Wi-Fi. (n.d.). Retrieved from https://www.antamedia.com/maritime-Wi-Fi/
32) Remote Configuration Service. (n.d.). Retrieved from https://www.kongsberg.com/maritime/services/kongsberg-remote-services/remote-configuration-service/
33) What is Social Engineering. (n.d.). Retrieved from https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering
34) Phishing. (n.d.). Retrieved from https://csrc.nist.gov/glossary/term/phishing
35) Fleet Mail. (n.d.). Retrieved from https://www.inmarsat.com/en/solutions-services/maritime/services/fleet-mail.html
36) GTMailPlus. (n.d.). Retrieved from https://www.gtmaritime.com/services/gtmailplus/
37) Unpatched Software Security Risk. (n.d.). Retrieved from https://www.arcserve.com/blog/unpatched-software-security-risk
38) Maritime Managed IT Services. (n.d.). Retrieved from https://marpoint.gr/maritime-managed-it-services/
39) IMO2021. (n.d.). Retrieved from https://imo-2021.com/imo2021
40) Cyber Security Elearning. (n.d.). Retrieved from https://www.dnv.com/maritime/maritime-academy/cyber-security-elearning.html
41) Resolution MSC.428(98) [PDF]. (2017, June 16). Retrieved from https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf
42) Maritime Cyber Security Awareness. (n.d.). Retrieved from https://www.lr.org/en/services/business-advisory/training/understanding-rules-and-regulations/maritime-cyber-security-awareness2/
43) Industry Standard Software Maintenance of Shipboard Equipment. (2017, December). Retrieved from https://www.bimco.org/about-us-and-our-members/publications/industry-standard-software-maintenance-of-shipboard-equipment
44) What is Malware? (n.d.). Retrieved from https://www.cisco.com/site/us/en/products/security/what-is-malware.html
45) Cheerala, R., & Kaur, G. (2021). A Comprehensive Study on Malware Detection and Prevention Techniques used by Anti-Virus. Retrieved from https://ieeexplore.ieee.org/abstract/document/9445322
46) Dualog Endpoint. (n.d.). Retrieved from https://www.dualog.com/services/endpoint
47) GTSentinel. (n.d.). Retrieved from https://www.gtmaritime.com/services/gtsentinel/

48) EI-ISAC Cybersecurity Spotlight: Password Attacks. (n.d.). Retrieved from https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-password-attacks
49) Two-Factor Vessel Authentication Service. (n.d.). Retrieved from https://sgsmarttech.com/two-factor-vessel-authentication-service.html
50) RFC 6284. (n.d.). Retrieved from https://datatracker.ietf.org/doc/html/rfc6284
51) Satheesh, M., & Deepika, M. (2020). Implementation of Multifactor Authentication Using Optimistic Fair Exchange. Journal of Ubiquitous Computing and Communication Technologies. Retrieved from https://irojournals.com/jucct/V2/I2/02.pdf
52) RANSOMWARE. (n.d.). Retrieved from https://www.trendmicro.com/vinfo/us/security/definition/RANSOMWARE
53) What is a Denial of Service Attack (DoS)? (n.d.). Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos
54) What is Remote Access Trojan? (n.d.). Retrieved from https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-remote-access-trojan/
55) Zhang, J., & Li, H. (2017). Research and Implementation of a Data Backup and Recovery System for Important Business Areas. Retrieved from https://ieeexplore.ieee.org/abstract/document/8048193
56) Resilio Connect. (n.d.). Retrieved from https://www.resilio.com/industries/marine/
57) Cisco. (n.d.). Configuration of Denial of Service Prevention Techniques on Cisco Small Business 500 Series Stackable Managed Switches. Retrieved from https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-500-series-stackable-managed-switches/smb2598-configuration-of-denial-of-service-prevention-techniques-sec.html
58) Zscaler. (n.d.). What is Network Segmentation? | Zscaler. Retrieved from https://www.zscaler.com/resources/security-terms-glossary/what-is-network-segmentation
59) Security Awareness Training: Network Segmentation. (n.d.). Retrieved from https://www.comptia.org/blog/security-awareness-training-network-segmentation
60) Redundancy. (n.d.). Retrieved from https://iadclexicon.org/redundancy/
61) Legacy Application or System. (n.d.). Retrieved from https://www.gartner.com/en/information-technology/glossary/legacy-application-or-system
62) Supply Chain Attacks. (n.d.). Retrieved from https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/
63) System Interconnection. (n.d.). Retrieved from https://csrc.nist.gov/glossary/term/system_interconnection#:~:text=A%20direct%20connection%20between%20two,%2C%20information%20services%2C%20and%20resources
64) Cisco. (n.d.). Cisco TrustSec | Network Segmentation | Cisco. Retrieved from https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html
65) Karatisoglou, M., Farao, A., Bolgouras, V., & Xenakis, C. (2022, June). BRIDGE: BRIDGing the gap bEtween CTI production and consumption. In 2022 14th International Conference on Communications (COMM) (pp. 1-6). IEEE.
66) CyberOwl. (n.d.). Retrieved from https://cyberowl.io/
67) Fortinet. (n.d.). Snort - Network Intrusion Detection & Prevention System (IDS/IPS). Retrieved from https://www.fortinet.com/resources/cyberglossary/snort
68) Kalderemidis, I., Farao, A., Bountakas, P., Panda, S., & Xenakis, C. (2022, August). GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-9).