Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

RENÉ SØRENSEN

How to Improve the Cyber Security Awareness in The Shipping Industry

DEGREE PROGRAMME IN MARITIME MANAGEMENT
2023

ABSTRACT

Sørensen, René: How to Improve the Cyber Security Awareness in The Shipping Industry
Master's thesis
Degree Programme in Maritime Management
December 2023
Number of pages: 70

In an era of increasing digital connectivity, the maritime industry plays a critical role in global trade. However, this reliance on advanced technology also exposes the industry to potential cyber threats. The thesis delves into the concerns surrounding cyber security in the maritime industry and proposes strategies to enhance cyber security awareness. The thesis discusses the background and context of cyber security in the maritime industry, highlighting the growing interconnectivity and reliance on digital systems. It identifies the problem statement as the need to enhance the cyber security awareness to safeguard maritime operations against cyber threats, protect critical systems, and ensure crew safety. The research objectives are outlined, which include assessing cyber security awareness among seafarers, assessing current cyber security measures, identifying cyber threats and vulnerabilities, and proposing strategies for risk assessment and mitigation. A thorough review of the literature is conducted, covering topics such as cyber security in the maritime industry, vulnerabilities, cyber threats, and attack vectors, reported cyber security breaches, existing cyber security measures and frameworks, and challenges in current practices. The methodology section explains the research design and data collection methods used in the study, while emphasizing ethical considerations and the question of data reliability. The findings and analysis section presents the data collected and provides an in-depth analysis of the results. This includes a survey that examines the current cyber security awareness among seafarers, methods for identifying and assessing cyber risks, and strategies for mitigating them. The effectiveness of these strategies is evaluated, and recommendations for enhancing cyber security awareness are proposed. The thesis emphasizes the significance of the study, highlighting its potential to raise awareness, promote effective cyber risk management, and contribute to the academic and professional literature on cyber security in the maritime industry. It acknowledges the limitations of the study, such as availability of data and evolving cyber threats because of global technological development. In conclusion, this thesis serves as a comprehensive overview of cyber security awareness in the shipping industry, addressing the challenges and vulnerabilities, evaluating existing measures, and proposing strategies to enhance cyber security awareness among seafarers. It emphasizes the importance of ongoing risk assessment, proactive measures, and collaboration within the industry to ensure the safety and security of maritime operations.

Keywords: Cyber Awareness, Cyber Security, Risk assessments, Mitigation Strategies, Guidelines, Regulatory Frameworks, Knowledge sharing.

CONTENTS

ABBREVIATIONS

AIS – Automatic Identification System

BIMCO – Baltic and International Maritime Council

CBS – Computer Based Systems

COTS - Commercial-off-the-shelf products

DNV – Det Norske Veritas (Classification Society)

DOS – Denial of Service

ECDIS – Electronic Chart Display and Information System

GNSS – Global Navigational Satellite System

IACS – International Association of Classification Societies

IMO - International Maritime Organization

ISM – International Safety Management

ISMS – Information Security Management System

IT – Information Technology

OT – Operational Technology

SDLC – Secure Development Lifecycle

VPN – Virtual Private Network

1 INTRODUCTION

1.1 Background and context of cyber security in the maritime industry

The maritime industry plays a vital role in global trade and transportation, serving as the lifeline for most of the world's trade. As the industry has become increasingly reliant on advanced information technology and operational technology systems, it has also become a potential target for cyber threats. With the proliferation of digital connectivity and the integration of systems and networks, the maritime industry faces significant cybersecurity challenges that must be addressed. This section provides a comprehensive background and context of cybersecurity in the maritime industry. It explores the implications of increasing connectivity, digitalization, and automation on ship operations and the overall security of the industry. It delves into the risks and vulnerabilities associated with the integration of IT and OT systems, highlighting the potential consequences of cyber threats on the safety, efficiency, and reliability of maritime operations. The section also examines the regulatory landscape and industry standards relevant to cybersecurity in the maritime sector. It discusses the guidelines and recommendations put forth by international organizations, such as the International Maritime Organization (IMO) and the International Association of Classification Societies (IACS), to promote cyber resilience and risk management within the industry. By understanding the background and context of cybersecurity in the maritime industry, stakeholders can gain insights into the challenges and complexities associated with protecting critical systems and data. This understanding serves as a foundation for developing effective strategies and measures to mitigate cyber risks and enhance cybersecurity awareness among seafarers and maritime organizations.

1.2 Problem statement and research objectives

Problem statement:

How to Improve the Cyber Security Awareness in The Shipping Industry

The project aims to create cyber security awareness and understand the aspects of cybersecurity measures within the maritime industry, considering the increasing interconnectedness and digitalization of ship systems and networks. It will aim at providing an understanding of the potential cyber threats and attack vectors that is faced by ships while evaluating existing cybersecurity measures and proposing a framework which is made to address the specific needs and requirements of ship operations. By diving into this topic, the project aims to contribute to knowledge and understanding of cyber security in the maritime industry. It also aims to identify practical recommendations for enhancing cybersecurity practises on board ships and promote the adoption of effective cybersecurity measures to mitigate cyber risks in ship operations.

1.3 Research objectives

- Assessing cybersecurity awareness among seafarers.
- Assess the existing cyber security measures and frameworks in the maritime industry.
- Identify cyber threats and attack vectors that pose risks to ship operations and critical systems on board.
- Address the challenges and vulnerabilities in the current cyber security measures.
- investigate the cybersecurity awareness measures amongst seafarers and highlight the significance in maintaining operational reliability and crew safety on board.
- Enhance the understanding of cyber risks and identify effective cybersecurity practises within the maritime industry.

- Identify OT and IT systems and their importance in ship operations.

1.4 Significance of the study

The study carries substantial importance in relation to the ever-evolving digital era. The increased dependence on technology inevitably exposes maritime operations to potential cybersecurity threats, which, if not appropriately addressed, could lead to severe disruptions in global trade, safety issues, environmental damage, and significant financial losses as seen in the NotPetya Incident. One critical aspect of the study is its potential to heighten the awareness of cybersecurity threats within the maritime industry and its operations. By understanding the types of risks, their sources, and their potential impacts, stakeholders in the industry can begin to approach their operations with an increased sense of caution and vigilance. This heightened awareness is a crucial first step in producing a proactive culture of cybersecurity within the industry. The study also carries significant implications for the development and implementation of effective cybersecurity strategies in the maritime industry. By identifying the most common and most dangerous threats to cybersecurity in maritime operations, the study will provide valuable information that can be used to identify various important cybersecurity protocols and measures specifically for these threats. Additionally, the study also focus on mitigating and assessing cybersecurity risks and their importance of being mitigated. Through this study, maritime operatives can understand effective methods to reduce the likelihood or impact of cybersecurity threats and how to assess their readiness and response to these threats. These insights could potentially contribute to enhancing the overall cybersecurity posture of the maritime industry. Lastly, this study will also contribute to the academic and professional literature on cybersecurity in the maritime industry. This contribution is significant because it expands the knowledge base, creating a resource that future researchers, maritime operatives, and policy makers can draw upon when considering their cybersecurity strategies. In conclusion, the importance of this study lies not just in its immediate practical applications, but also in its potential

to shift the mindset of the maritime industry towards a more security-conscious and proactive approach to cybersecurity.

1.5 Scope and limitations

1.5.1 Scope

The scope of this study will be to understand whether the shipping industry needs to improve the cybersecurity awareness in the industry and what is the current level of cyber security awareness. This will involve Identifying the current cybersecurity risks that are prevalent in ship operations, including both IT and OT systems by defining them and their functions. This will involve a detailed review of the current literature on the topic, as well as using questionnaires to investigate the current apprehension on cybersecurity in the industry. It will also be important to propose and evaluate potential mitigation strategies for these risks through the research and questionnaires. This will involve the identification of various protocols, training programs, and technological solutions aimed at reducing the impact of these risks. Assessing the mitigation strategies and their functions is also important in this context. This will involve a combination of the collected data and already existing mitigation guidelines and a quantitative approach to evaluate how well these strategies perform in a real-world context. How much does the seafarers already know? And what do they need to know? Developing an understanding of the different guidelines and frameworks used in the industry for ongoing risk assessment in the field of ship operations. This will involve identifying legal framework, guidelines, or best practices for identifying and managing cybersecurity risks.

1.5.2 Limitations

The study will be limited by the availability and willingness of industry stakeholders to participate in interviews and provide relevant qualitative insight. Some organizations may be reluctant to share sensitive information about their cybersecurity practices and vulnerabilities. Whereas the conducted survey and

literature review will be the primary data for the analysis of the thesis. The rapidly evolving nature of cyber threats means that the study's findings may become less relevant over time. The study will attempt to address this by focusing on fundamental principles of risk identification and mitigation and identifying specific threats but knowing that these threats can change in a short period of time. The mitigation strategies will be identified and assessed through thorough analysis and by comparing different guidelines and mitigation strategies. The study's recommendations will be based on current technology and industry practices. Changes in technology or regulatory requirements could impact the feasibility or effectiveness of these recommendations. The study will focus on the shipping industry, and its findings may or may not be applicable to other industries with similar cybersecurity concerns. The study has a large amount of research objectives, and it will be difficult to go too much into detail with these objectives without losing track on the actual aim, which is to create further cybersecurity awareness.

2 OVERVIEW OF CYBER SECURITY IN THE MARITIME INDUSTRY

2.1 Definition and scope

The BIMCO guidelines can assist in getting an overview of cyber security in the maritime industry and assist in defining what cyber security means in the context of the maritime industry and explaining its importance and significance. This includes outlining the potential threats and vulnerabilities specific to maritime operations. In this connection we need to divide the definition and scope into IT and OT systems. IT systems and OT systems are two distinct types of systems found onboard ships. However, its important bearing in mind that BIMCO is only providing a guideline and therefore the legal framework in this thesis has higher significance without neglecting the importance of BIMCO Guidelines.

2.2 IT Systems

The BIMCO guidelines explains IT systems, also known as Information Technology systems, include the hardware and software that manages and processes data. These systems are typically used for tasks related to communication, data storage, and information management on board. Some examples of IT systems include computers, servers, networking equipment, email systems, and software applications such as the safety management systems and planned maintenance systems being the most vital for the safe operation of the ships. IT systems are connected to the internet and are vulnerable to cyber threats such as malware, hacking, and data breaches. [1]

2.3 OT Systems

OT systems refer to Operational Technology systems. These systems are responsible for monitoring and controlling physical devices, processes, and events within the ship. OT systems are employed in various critical functions onboard, such as propulsion and machinery management, power control systems, navigation systems, and access control systems. Unlike IT systems, OT systems are not typically connected to the internet and have limited interaction with external networks. However, they can still be vulnerable to cyber incidents if proper security measures are not in place. The main difference between IT and OT systems lies in their primary function and level of connectivity. IT systems focus on managing and processing information, while OT systems are responsible for operating and controlling physical equipment and processes. Both types of systems play essential roles onboard ships, and it is crucial to ensure their security to protect against cyber threats.[2]

[1] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020)
[2] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020) Page 7

3 CYBER THREATS AND ATTACK VECTORS IN SHIP OPERATIONS

3.1 The stages of a cyber attack

To understand cyber threats and attack vectors you need to understand the stages of a cyber-attack. A cyber-attack can as an example consist of survey/reconnaissance where the attackers are luring to find a potential vulnerable target. The target could be a seafarer, a shipping office ashore or a ship or a fleet of ships. Next stage is where the target has been located and the attack is delivered, which breaches the target system and later it will attack other underlying systems within the main target systems. Loading and discharging programs can be potential targets for the attackers, and this can cause disruption in the ship operations. Once there has been a breach in the on-board cybersecurity system then there is potential for attacks in the navigational systems, which are vital for the safe operations of the vessel. Lastly there is the pivot stage where an attacker uses an already compromised system to attack other systems that are connected to the same network. [3]

3.2 Motivation and objectives of cyber attackers

The motivation and objectives of the attacker determine the impact and outcome for the company or ships data and systems. Some motivations consist of:

- Access to sensitive and commercial data, which can be sold to competitors.
- Manipulation of data and systems with the intention of harming the vessel and company.
- Demanding a ransom for the data the attackers have obtained.
- Disruption of all normal ship operations.[4]

[3] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020)
[4] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020) Page 14

3.3 Threat Actors

The threat actors that may target ships which include accidental actors are, activists, criminals, opportunists, states, state sponsored organizations and terrorists. Each of these actors may have different motivations and objective for conducting cyber- attacks. These motivations can consist of economy, political, ideological, operational, or competitive motivations.[5]

3.4 Types of Cyber Threats

According to the "BIMCO -The Guidelines on Cyber Security Onboard Ships"[6] cyber threats are put in to 2 categories. Untargeted and targeted attacks. Untargeted attacks are typically widespread and use tools and techniques available on the internet to exploit potential vulnerabilities.

3.5 Untargeted attacks consist of the following:

Malware: (Malicious Software)
Water Holing: (Fake Website)
Scanning: (Searching the internet for potential vulnerabilities)
Typo squatting: (Websites relying on type errors from users).

3.6 Targeted attacks consist of the following:

Social engineering: Its intention is to manipulate people to make security breaches typically through interaction on social media. (click-bait)

Brute force: Checking all possible passwords until the password is correct and thereby security is breached.

---

[5] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020) Page 13
[6] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020) Page 13

Credential stuffing. Using common or previously used passwords to attempt gaining unauthorized access to a system or application.

DOS: Denial of service (DoS) prevents legitimate and authorized users from accessing information, usually by flooding a network with data. This attack can take control of several computers.

Phishing: Sending emails to many potential targets asking for pieces of sensitive or confidential information. The mail can consist of links which also consist of Malware.

Spear-phishing: Like phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software. Sat-C systems have been used for this type of attacks. [7]
Targeted attacks are specifically aimed at a company or ships system and data.

4 EVALUATION OF VULNERABILITIES AND POTENTIAL IMPACTS ON CRITICAL SYSTEMS

When looking at vulnerabilities it is important to identify the systems on board that are vulnerable in connection with maritime operations.
These systems consist of: Cargo and loading management systems, Bridge systems such as ECDIS, GNSS or AIS systems, Propulsion and machinery systems, Safety management systems, planned maintenance systems and all computers that are network connected on board.

[7] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020)

4.1 Vulnerabilities

IT and OT vulnerabilities can be exploited by attackers to disrupt ship operations or other relevant operations in the maritime industry. Disruptions can cause delays in loading and discharging operations or unsafe ship operations caused by disrupting vital systems like navigational or propulsion systems.
An attack in the planned maintenance system can cause disruption in the daily management of the maintenance and an attack to the safety management systems can create risks in the daily work tasks onboard. All these systems are therefore vital for the safe operation of the ships. There are several common vulnerabilities that can affect critical systems onboard ships. Obsolete and unsupported operating systems refers to the use of outdated operating systems that are no longer receiving updates or support from the manufacturer. These systems may have known vulnerabilities that can be exploited by attackers. Another vulnerability is unpatched system software. If you fail to apply software updates and patches this will leave systems vulnerable to known security flaws. These updates often contain bug fixes and security patches that address vulnerabilities. Outdated or missing antivirus software and protection from malware is another risk. Without up-to-date antivirus software and robust protection from malware, ships are at risk of infection by malicious software, such as viruses, worms, and ransomware. Another risk is Inadequate security configurations and best practices. Poorly configured networks and systems, along with the use of default administrator accounts and passwords, can create weaknesses that can be exploited by attackers. Another potential risk is Insufficient access controls. If the access control is insufficient, it will make it easier for unauthorized individuals, such as contractors or service providers, to gain access to critical systems and sensitive data. It is therefore of vital importance to manage this. The lack of awareness and training among staff members can also lead to cybersecurity best practices not being followed, increasing the risk of successful attacks. The importance of contingency plans is also vital to mention. Missing, inadequate, or untested contingency plans and procedures are a risk that needs to be addressed. Inadequate or nonexistent contingency plans and procedures can hinder the response and recovery efforts in the

event of a cyber incident, making it difficult to mitigate the impact and restore normal operations.[8]

4.2 The Impacts on critical systems

The impact of these vulnerabilities on critical systems can vary depending on the specific system and the nature of the attack. However, potential impacts include disruption of system operations. When disrupting the system operations, attackers may be able to interrupt or manipulate critical systems, leading to a loss of functionality and potential safety risks. Risk of collision, unsafe navigation, grounding, positioning errors in Dynamic Positioning systems etc. Another vulnerability is the risk of unauthorized access to sensitive data. Breaches in cybersecurity measures can result in unauthorized access to commercially sensitive or confidential information, posing risks to the company's operations, reputation, and compliance. Hence the importance of having IT policies on bord to mitigate risks from 3rd party visitors. Another vulnerability is manipulation of important information. Here the Attackers may alter critical information such as cargo manifests, loading lists, or stow plans, potentially leading to cargo mismanagement, fraudulent activities, or safety hazards. This can cause the company to make mistakes that are vital for the commercial reputation and for its financial turnover. Another vulnerability can be the unavailability/denial of service (DOS). In some cases, cyber incidents can lead to a complete unavailability or denial of service, rendering systems inaccessible or non-operational, disrupting normal business operations. This can also be very damaging to a business and its reputation. In conclusion cyber incidents can result in significant financial losses, including repair costs, operational delays, and potential legal or regulatory consequences. Public exposure of security breaches can also damage a company's reputation. [9]

[8] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020) Page 17 - 21

[9] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020)

5 GUIDELINES

5.1 BIMCO Guidelines

When creating an overview of cyber security measures in the maritime industry it is important to discuss the regulations, guidelines and initiatives that relates to maritime cybersecurity. The document “The Guidelines on Cyber Security Onboard Ships” by BIMCO among others[10] mentions relevant guidelines, regulations and standards that are issued by international organizations and regulatory institutions such as the International Maritime Organization IMO. It is produced and supported by various organizations including BIMCO, Chamber of Shipping of America, Digital Containership Association, and others. The purpose of these guidelines is to improve the safety and security of seafarers, the environment, the cargo, and the ships in the maritime industry. It aims to assist in the development of a proper cyber risk management strategy onboard ships, focusing on work processes, equipment, training, incident response, and recovery management. The guideline explains the characteristics of cyber security in the maritime industry and the importance of protecting IT, OT, information, and data from unauthorized access, manipulation, and disruption. It highlights the potential cyber vulnerabilities and risks that arise from increased connectivity in the industry. The guidelines emphasize the need for senior management involvement in cyber risk management and highlight the roles, responsibilities, and tasks of different stakeholders in the company. It emphasizes the importance of evaluating the likelihood and threat, along with the impact and vulnerabilities, when assessing cyber risk. The guideline covers the identification of threats, including various threat actors and their motivations and objectives. It explains the different types of cyber threats, such as malware, social engineering, phishing, and denial of service attacks. It discusses the identification of vulnerabilities and common vulnerabilities that may be found onboard ships. This includes obsolete and unsupported operating systems, unpatched system software, inadequate security configurations, and

[10] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020)

inadequate access controls, among others. The guidelines also highlight the importance of documenting IT and OT systems, including creating an asset register and logical maps of networks. It emphasizes the need for an inventory of communicating devices and software, as well as the inventory of network services for each equipment. Lastly, the guideline emphasizes the importance of continuous monitoring, periodic risk assessments, and the development and implementation of relevant plans and procedures. It discusses the criticality of contingency plans and the need to respond to and recover from cyber security incidents effectively. Overall, this guideline can be used to create an overview of cyber security in the maritime industry by providing guidance on identifying threats and vulnerabilities, assessing risk, developing protection and detection measures, and establishing contingency plans. It helps companies in the industry to implement a comprehensive cyber risk management strategy to safeguard their operations and mitigate potential cyber threats.[11]

6 REGULATORY FRAMEWORK AND THEIR PURPOSE

6.1 IACS Recommendation 166

The regulatory framework outlined in the IACS framework is designed to provide technical information and guidance to stakeholders involved in the construction and operation of cyber resilient ships. The purpose of this framework is to ensure that ships are equipped with computer-based systems that can effectively cope with cyber incidents throughout their service life. Resilience, in this context, refers to the ability of these systems to prevent and mitigate cyber incidents, ultimately ensuring the safety of the crew, the vessel, and the marine environment. This recommendation supports the International Maritime Organization's (IMO) Resolution MSC.428(98), which emphasizes the importance of addressing cyber risks in safety management systems. It also

[11] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020)

aligns with the IACS UR E26 standards on the cyber resilience of ships which is mentioned in the thesis as well. The framework is organized into several sections, including scope, reference guidelines and standards, terms and definitions, goals for design and construction, functional requirements, technical considerations, and verification testing. Key elements of the framework include identifying and understanding the devices, systems, networks, and data flows on board, implementing secure configurations and integration of computer-based systems, detecting, and responding to cyber incidents in a timely manner, and ensuring the ability to recover and restore system functionality. Additionally, measures are provided for asset identification, network segmentation, physical access control, software assurance, and more.

Overall, this regulatory framework aims to enhance the cyber resilience of ships and promote the secure operation and protection of computer-based systems, ultimately mitigating the risks associated with cyber threats and ensuring the safety of the vessel, crew, and marine environment.[12]

6.2 E26 Cyber Resilience of Ships

The purpose of this framework is to provide a set of requirements and guidelines for ensuring the cyber resilience of ships. It recognizes that with the increasing interconnection of computer systems on ships and the use of commercial-off-the-shelf (COTS) products, there is a heightened risk of cyber-attacks that can affect personnel data, personal safety, the safety of the ship, and the marine environment. The framework aims to establish a common set of minimum functional and performance criteria to deliver a ship that is cyber resilient. It emphasizes the need for consistent and comprehensive measures to safeguard ships from current and emerging threats. The International Association of Classification Societies (IACS) considers a goal-based approach applied consistently across the full threat surface to be necessary for achieving cyber resilient ships. The framework is structured to address different aspects of cyber resilience, including identification, protection, detection, response, and recovery. It provides requirements for inventorying CBSs and networks

[12] (Societies I. i.-1., 2020)

onboard, creating security zones, implementing network protection safeguards, using antivirus and malware protection, enforcing access control measures, managing wireless communication, and controlling remote access. Additionally, the framework emphasizes the importance of incident response planning, controlled shutdown and recovery procedures, and the need for backup and restore capabilities. Lastly It also highlights the significance of performance evaluation and testing, which are carried out based on a comprehensive test plan to ensure the effective implementation of the cyber resilience measures. The overall goal of the framework is to support safe and secure shipping by effectively managing cyber risk through the implementation of appropriate measures and procedures.[13]

6.3 E27 Cyber resilience of on-board systems and equipment

The purpose of this framework is to specify unified requirements for the cyber resilience of on-board systems and equipment in the maritime industry. With the increasing reliance on Operational Technology (OT) and Information Technology (IT) in vessels, ports, and container terminals, there is a growing risk of cyber-attacks that can affect business operations, personnel data, human safety, the safety of the ship, and even pose risks to the marine environment. It is therefore necessary to establish a common set of minimum requirements to ensure that systems and equipment on board can withstand cyber threats and maintain their functionality. The framework covers various aspects related to cyber resilience, including the general introduction, limitations, scope, definitions, and abbreviations. These requirements also addresses the security philosophy, documentation requirements, system requirements, and product design and development requirements. These requirements aim to enhance the cyber resilience of on-board systems and equipment, ensuring that they can withstand cyber-attacks, protect sensitive information, maintain essential functions, and recover from disruptions or failures. By implementing these

[13] (Societies I. I., 2022)

requirements, the maritime industry can better safeguard shipping operations and mitigate the risks associated with cyber threats.[14]

6.4 IMO Maritime Cyber Risk Management in Safety Management Systems

The purpose of this framework, which is Resolution MSC.428(98), is to address the urgent need for maritime cyber risk management in safety management systems. It emphasizes the need to raise awareness about cyber threats and vulnerabilities to ensure safe and secure shipping. The framework recognizes that various stakeholders in the maritime industry, such as Administrations, classification societies, shipowners, ship operators, equipment manufacturers, service providers, ports, and port facilities, should work together to safeguard shipping from existing and emerging cyber threats. It also acknowledges the Guidelines on maritime cyber risk management approved by the Facilitation Committee and the Maritime Safety Committee, which provide recommendations for incorporating cyber risk management into existing risk management processes. The framework highlights the importance of the International Safety Management (ISM) Code, which governs safe ship operation and environmental protection, and affirms that approved safety management systems should consider cyber risk management. It encourages Administrations to address cyber risks in safety management systems by the first annual verification of a company's Document of Compliance after 1 January 2021. The framework also acknowledges the need for confidentiality in certain aspects of cyber risk management and requests Member States to bring this resolution to the attention of all stakeholders. [15]

6.5 IMO Guidelines on Maritime Cyber Risk Management

The purpose of this IMO guideline is to provide high-level recommendations and guidance on managing cyber risks in the maritime industry. The document recognizes the increasing reliance on digitization, integration, automation, and

[14] (internatioal association of classification societies, 2022)
[15] (MSC.428(98), 2017)

network-based systems in shipping, and highlights the urgent need to raise awareness on cyber risk threats and vulnerabilities. The framework aims to safeguard shipping by addressing the current and emerging cyber threats and vulnerabilities related to the use of technology assets in the maritime sector. It emphasizes the importance of protecting information and systems from being corrupted, lost, or compromised, which could lead to operational, safety, or security failures. The guidelines provide functional elements that support effective cyber risk management, covering the identification of personnel roles and responsibilities, protection measures, detection of cyber events, response and resilience planning, and recovery measures. These elements are meant to be implemented concurrently and continuously to ensure a proactive and holistic approach to managing cyber risks. Furthermore, the framework stresses the need for senior management to embed a culture of cyber risk awareness throughout the organization and to establish a flexible and continuously evaluated cyber risk management regime. It also encourages organizations to assess their current cyber risk management posture and develop a risk-based approach to address any gaps or vulnerabilities. Overall, the purpose of this document is to provide a framework for organizations in the shipping industry to effectively manage cyber risks and promote safe and secure shipping operations in the face of evolving cyber threats.[16]

6.6 ISO Standards

ISO 27001 and ISO 27002 are international standards that provide guidelines and best practices for information security management. ISO 27001 is a comprehensive framework that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) within an organization. The purpose of ISO 27001 is to help organizations protect their information assets and manage the associated risks effectively. It provides a systematic approach to identifying, assessing, and managing information security risks, ensuring confidentiality, integrity, and availability of information. ISO 27002, on the other hand, is a

[16] (International Maritime Organisation, 2022)

companion standard to ISO 27001. It provides a set of controls and best practice recommendations for implementing and maintaining an information security management system. ISO 27002 covers a wide range of topics, including information security policies, organization of information security, asset management, human resource security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, incident management, business continuity management, and compliance. In summary, ISO 27001 sets the requirements for an information security management system, while ISO 27002 provides the detailed guidance on implementing those requirements and best practices for information security management. Together, these standards help organizations establish a robust and effective information security management framework to mitigate risks and protect sensitive information. [17]

6.7 Risk Management

The overview also helps with understanding the importance of risk management in maritime cybersecurity. This includes identifying vulnerabilities, risk assessing and implementing appropriate controls and counter measurements to mitigate the risks involved. The overview can also help to emphasize a need for continuous monitoring and incident response in connection with cybersecurity on board ships.[18],[19]

[17] (Calder, 2005)
[18] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020) page 3.
[19] (MSC.428(98), 2017)

7 AWARENESS AND TRAINING

In awareness and training focus is on the implementation of certain procedures to enhance cyber security onboard ships. These measures aim to address vulnerabilities and mitigate the risk of cyber incidents. Companies should provide cyber security awareness training to personnel at all levels, including shipboard crew. Training could cover topics such as recognizing phishing emails, proper password hygiene, and reporting suspicious activities. One cyber vital measure to implement is having an incident response plan. It is vital to have a well-defined incident response plan in place. This plan should outline the actions to be taken in the event of a cyber incident, including communication channels, roles and responsibilities, and steps for containment, investigation, and recovery. Another vital measure is to carry out Change Management. Proper change management procedures should be implemented to ensure that any changes to IT or OT systems are properly tested, approved, and documented. This helps prevent unauthorized changes that could introduce vulnerabilities. Proper access control is obviously also very important. Companies should establish access controls to limit user privileges and ensure that only authorized personnel have access to critical systems and data. This includes implementing strong password policies, regularly reviewing user access rights, and monitoring for unauthorized access attempts. A very important tool to make use of is security awareness campaigns. Regular security awareness campaigns should be conducted to educate personnel about the importance of cyber security and to promote a culture of security throughout the organization. Physical security measures should also be implemented to protect IT and OT infrastructure from unauthorized access. This may include measures such as securing server rooms, restricting physical access to critical systems, and properly disposing of sensitive information. Lastly Third-Party Management is also a very vital part of the awareness training. Companies should assess the cyber security capabilities of their third-party vendors and service providers. This includes conducting due diligence checks and establishing contractual requirements that align with the company's cyber security standards. By implementing these procedural protection measures, companies can enhance

their cyber security posture and reduce the risk of cyber incidents onboard ships. (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020)[20] DNV has produced a report which underlines BIMCOs thesis regarding the importance of training personnel. According to DNV improper training will make personnel unaware actors in enhancing cyber-threats or "'friendly threat actors'" as DNV calls it. DNV recognizes a carelessness when we are untrained and unaware of the risks involved in cyber-attacks. There needs to be more training made available for the staff. Training which is of a higher quality, and which is properly planned and being done on a regular basis will according to DNV heighten the quality of the personnels cyber security awareness. [21]

7.1 Collaboration and information sharing

According to DNV it is important to Identify the potential significance and value of collaboration and information sharing between government agencies, port authorities, ship operators and cybersecurity experts. There are significant values in sharing information about threats, attacks, and best practices to enhance the overall posture of the maritime industry. According to the research conducted by DNV, only 31% of maritime professionals believe that organizations within the sector are effective at sharing information and lessons learned about cyber security risks, threats, and incidents. The lack of effective information sharing within the industry hampers the development of industry standards and best practices for cyber security. DNV emphasizes the importance of better information-sharing and collaboration among maritime organizations. It suggests that open discussion and sharing of experiences and challenges would benefit the industry, enabling organizations to learn from each other's successes and failures. Such knowledge-sharing will help in the development

[20] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020) page 34-38

[21] (Veritas, 2023) page 36

of industry standards and guidelines that can guide organizations in building a strong and effective cyber security posture. Furthermore, DNV highlights the need for a more risk-aware workforce and a cyber-secure culture. Effective training programs should be implemented to ensure that employees are well-informed about cyber security risks and best practices. This will help in minimizing human errors and inadvertent cyber risk within organizations. Overall, DNV emphasizes the importance of collaboration, information-sharing, and training as key recommendations for the maritime industry to enhance its cyber security capabilities and address the challenges it faces in this domain.[22]

7.2 Future Trends

At last, an overview of the overall cybersecurity topic may touch emerging trends in the industry that have potential implications for cybersecurity, this could be the increase in automation (autonomous vessels), Internet requirements of the future and other automation related challenges. The purpose of creating an overview of cybersecurity in the maritime sector is to provide short and simple yet informative summary of the key aspects and considerations related to cybersecurity within the maritime industry.

8 REPORTED CYBER SECURITY BREACHES AND THEIR IMPACT ON SHIP OPERATIONS

The NotPetya cyber incident, which occurred in June 2017, had significant impacts across industries worldwide, including the shipping industry. This ransomware attack was a wake-up call for many businesses about the potential vulnerability of their IT systems. The shipping industry, in particular, experienced severe consequences due to the NotPetya incident. Maersk, a global leader in shipping and logistics, was one of the most severely affected companies. It's estimated that the attack cost Maersk between $250 million and $300

[22] (Veritas, 2023) Page 35

million. Maersk's operations were severely disrupted. The ransomware infected and shut down the company's computer systems across 130 countries, making it impossible for the company to manage its 76 port and terminal operations. As a result, the company was unable to process orders and had to revert to manual processes, causing significant delays in shipping and port operations. The impact on Maersk's finances was significant. The company experienced financial losses due to the disruption in operations. The cost of recovery, and the need for significant cybersecurity upgrades was substantial. The estimated cost range of $250 million to $300 million includes these elements. The incident also led to some reputational damage for Maersk. The inability to fulfil shipping orders on time and the resultant chaos damaged customer trust in the company's reliability. However, some customers where quickly compensated to retain and restore the confidence in the company's performance. In the wake of the NotPetya incident, Maersk and other companies in the shipping industry had to invest heavily in cybersecurity measures to prevent similar incidents in the future, this includes updating and patching systems, training staff in cyber awareness, and implementing more robust security protocols. In hindsight it was identified that Maersk did not have the proper cyber security infrastructure needed to mitigate such an evasive cyberattack as NotPetya. Some servers were running on old Microsoft systems which was no longer supported or updated. It took Maersk 5 months before being back to fully normal operational standards. In conclusion, the NotPetya cyber incident had far-reaching implications for the shipping industry, highlighting the urgent need for robust cybersecurity measures in this increasingly digital sector. [23]

[23] (Greenberg, 2018)

9 CYBER SECURITY RISK IDENTIFICATION AND ASSESSMENT

BIMCO discusses the cyber security characteristics of the maritime industry. It emphasizes the importance of cyber security in protecting personnel, the ship, the environment, and the company's reputation. They highlight that cyber security is concerned with protecting IT and OT systems, as well as information and data, from unauthorized access, manipulation, and disruption.

The maritime industry faces specific vulnerabilities and risks due to its involvement in multiple stakeholder operations, use of legacy systems, online interface with shoreside parties, and reliance on remote monitoring and access to ship equipment. The sharing of sensitive information with shore-based service providers and the integration of various sub-systems from different vendors further compound the cyber risks. The chapter also underscores the growing use of digital solutions and in-creased connectivity within the industry, which presents both opportunities and challenges. While these advancements can improve efficiency, cost savings, and safety, they also increase the potential for cyber vulnerabilities and risks. To effectively manage cyber risks, companies are encouraged to embed a culture of cyber risk management at the senior management level and throughout the organization. This includes identifying the roles, responsibilities, and tasks of personnel involved in cyber risk management, as well as ensuring a holistic and flexible cyber risk governance regime. The International Maritime Organization (IMO) has also emphasized the im-portance of addressing cyber risk in safety management systems, encouraging administrations to ensure appropriate measures are in place. Additionally, guidelines from other associations, such as the International Association for Classification Societies, along with IMO provide further guidance on maritime cyber risk management. Overall, it is emphasized that there is a need for a comprehensive cyber risk management strategy that considers the specific characteristics and vulnerabilities of the maritime industry. The risks of facing a cyber-attack in ship operations or ashore does not seem greater, but the risks involved in the cyber-attack offshore can potentially be of greater consequence because of the human factor involved in ship operations. More and

more systems onboard are interacting with cyber-space and can therefore be potentially vulnerable for cyber-attacks. This can potentially cause harm to the crew, other equipment, or the environment. Harm that can seem far more severe than the one the onshore department might be facing[24].

9.1 Methods for identifying and assessing cyber security risks

Section 6 of the BIMCO guidelines focuses on risk assessment and how to produce one specifically for your vessel. Producing a risk assessment is an important step in managing cyber security on board ships. Risk assessments helps identify and evaluate potential risks and vulnerabilities that could affect the safety and security of the ship, crew, and cargo. Relationship between factors influencing risk. The guidelines emphasizes that risk is the product of multiple factors, including threat, vulnerability, and likelihood of an incident occurring. It highlights the importance of under-standing how these factors are interrelated and impact the overall risk level. [25]

9.2 Risk Assessment

The risk assessment process is divided into four phases:

Phase 1 is the preliminary risk assessment. This phase involves identifying and assessing potential risks before conducting a detailed analysis. It aims to provide an initial understanding of the risks and their potential impact on the company and its shipboard operations. The preliminary risk assessment helps in determining the priority level for conducting a detailed risk assessment. Phase 2 is the detailed risk assessment: In this phase, a comprehensive analysis of identified risks is conducted. It involves mapping threats and

[24] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020)
[25] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020)

vulnerabilities, evaluating the likelihood and impact of potential incidents, and determining the level of risk associated with each identified risk. The detailed risk assessment provides a more in-depth understanding of the risks and their potential consequences, allowing for better decision-making regarding risk mitigation and management strategies. Phase 3 is the risk evaluation and prioritization. Once the detailed risk assessment is completed, the identified risks are evaluated and prioritized based on their potential impact and likelihood. This phase helps in determining which risks pose the greatest threat to the company and its shipboard operations. It al-lows for the allocation of resources and implementation of appropriate risk management measures to address the most critical risks first. Phase 4 is the risk treatment and mitigation phase. In this final phase, risk treatment and mitigation strategies are developed and implemented to reduce the identified risks to an acceptable level. This may include the establishment of policies, procedures, and controls to address vulnerabilities, improve cyber security measures, and enhance incident response capabilities. Risk treatment and mitigation also involve ongoing monitoring and review of implemented measures to ensure their effectiveness in managing the identified risks. By following these four phases, companies can systematically assess, evaluate, and address the cyber security risks present in their shipboard operations, thereby enhancing the overall cyber resilience of their operations. [26]

9.3 Third-party risk assessment

Third-party risk assessments: This section highlights the importance of considering the cyber risk posed by third-party such as suppliers, and service providers that visits the ships. Companies should evaluate the cyber risk management processes and capabilities of these external parties and establish appropriate contractual agreements to address cyber security concerns. Overall, the guidelines provide guidance on conducting a thorough risk assessment to understand the cyber security risks specific to a ship and develop appropriate

[26] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020)

risk mitigation strategies on board. It underscores the im-portance of considering all relevant factors and engaging in continuous assessment to adapt to changing threats and vulnerabilities. [27]

9.4 Mitigating Cyber Security Risks

With the increasing reliance on advanced information technology and operational technology systems, the maritime industry has become vulnerable to cyber threats. The consequences of these threats can impact the safety, efficiency, and continuity of ship operations. Therefore, it is crucial to develop effective strategies for mitigating cybersecurity risks in ship operations.

9.4.1 IACS Mitigation Strategies

The recommendation from IACS proposes several strategies for ships to handle cyber incidents. IACS also recommends developing a contingency plan. This strategy is aligned with BIMCO. The ship-owner is responsible for developing a contingency plan that contains predetermined instructions or procedures for the crew to detect, respond, and limit the consequences of cyber incidents. The plan should also outline how the crew will recover the affected systems after ensuring the ship's safety. Another vital measure is the ability to detecting cyber-Incidents. The crew should be trained to detect cyber incidents and identify the failed system promptly so they can take proper action. Once a cyber incident is detected, the crew should determine effective response options and take appropriate actions to mitigate the impact of the incident. After securing the ship's safety, the crew should work on recovering the failed system to restore its functionality. Lastly It is essential to investigate and document cyber incidents to understand their causes, effects, and potential vulnerabilities. This information can help in improving future cyber resilience measures. These strategies aim to ensure that ships have the capabilities to effectively

[27] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020)

cope with cyber incidents and maintain their resilience throughout their service life. The reasons for choosing IACS Recommendation on cyber resilience is because it supports IMO Resolution MSC.428(98) and MSC-FAL.1/Circ.3, which require cyber risks to be addressed in safety management systems by a specific deadline. It aligns with IACS UR E26, which focuses on the cyber resilience of ships. The document provides an overview and a foundation of the structure, scope, reference standards, and terms and definitions related to cybersecurity in maritime operations. It serves as a roadmap and framework for developing a program for cyber resilient computer-based systems on board ships.

9.4.2 E26 Cyber resilience of ships and its mitigation strategies

This framework provides a set of requirements and guidelines aimed at mitigating cyber security risks in the context of ships. By implementing these requirements and following the outlined guidelines, shipowners, ship de-signers, shipyards, system integrators, suppliers, and classification societies can contribute to the cyber resilience of ships and reduce the occurrence and impact of cyber incidents. The framework emphasizes the importance of understanding and identifying the cyber security risks faced by ships. It provides guidance on conducting an inventory of computer-based systems (CBSs) and networks onboard, which helps identify vulnerabilities and potential points of entry for cyber-attacks. The framework also outlines requirements for establishing security zones, implementing network protection measures such as firewalls, and implementing safeguards against malicious code. These measures help protect CBSs and networks from unauthorized access, data breaches, and other cyber threats. The framework emphasizes the importance of continuous monitoring of networks and CBSs for anomalies and malfunctions. It encourages the use of intrusion detection systems and diagnostic functions to promptly detect and respond to any cyber incidents. The framework requires the development of an incident response plan that outlines procedures for responding to cyber security incidents. This includes instructions on how to detect, report, and mitigate the impact of incidents. It also emphasizes the importance of con-

trolled shutdown, restoration of minimal risk conditions, and collaboration with external support during incident response. The framework emphasizes the need for a recovery plan that supports the restoration of CBSs (Computer Based Systems) and networks to an operational state after a cyber incident. It emphasizes the importance of maintaining backups, testing their functionality, and having procedures in place for controlled shutdown, reset, roll-back, and restart of affected systems. Overall, this framework provides tools for stakeholders to implement measures and procedures that enhance the cyber resilience of ships, safe-guard personnel data, human safety, the safety of the ship, and the marine environment from cyber threats. By adhering to these requirements, stakeholders can effectively mitigate cyber security risks in the maritime industry.

9.4.3 E27 Cyber resilience of on-board systems and equipment and its mitigation strategies

This framework provides unified requirements for the cyber resilience of on-board systems and equipment. It is designed to address the cybersecurity risks associated with vessels, ports, container terminals, and other maritime operations. By implementing the requirements specified in E27, organizations can establish a common set of minimum cybersecurity measures to protect their systems and equipment from cyber threats. One important measure to implement is human user identification and authentication. By implementing this the company is ensuring that all human users accessing the system are properly identified and authenticated to pre-vent unauthorized access. Another important measure is to implement account management. Implementing controls for managing user accounts, including adding, modifying, disabling, and removing accounts by authorized users. Here a somewhat similar measure is Identifier management. Managing identifiers by user, group, and role to ensure appropriate access controls are in place. It is also important with authenticator management. Changing all default authenticators, protects authenticators from unauthorized access or modification, and implementing strong password requirements. Access management of wireless systems is another important

measure. Controlling and monitoring the use of wire-less communication is vital to prevent unauthorized access to the wireless systems. Protection of malicious codes is another measure which is vital to implement to provide suitable protection measures to prevent, detect, and mitigate the effects of malicious code or unauthorized software. Configuring the network and security settings according to recommended industry practices and guidelines is also vital to protect the networks from being compromised. Implementing processes and capabilities for system backup, recovery, and reconstitution to maintain operational continuity in the event of disruptions or failures. Implementing processes to identify, assess, and apply security patches and updates to address known vulnerabilities. Following a Secure Development Lifecycle (SDLC) to ensure that security aspects are addressed throughout the product design and development stages. This will help securing the development lifecycle. By adhering to these requirements and implementing appropriate cybersecurity controls, organizations can minimize the risk of cyber-attacks and protect the confidentiality, integrity, and availability of their systems, data, and operations. It provides a framework for ensuring cyber resilience and promoting safe and secure maritime operations.

9.4.4 ISO 27001 mitigation strategies

ISO 27001 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS). The key elements involved in using ISO 27001 are described in this section. Firstly, define the scope and policy of the ISMS implementation. It may include the entire organization or a specific division. Also, establish an information security policy that aligns with the organizational objectives and regulatory requirements. Secondly it is important to conduct a comprehensive risk assessment to identify threats and vulnerabilities that could impact the organization's information. This involves identifying assets, threats, vulnerabilities, impacts, likelihoods, and risk levels. Determine the appropriate methods to manage each risk identified. You can choose to accept, avoid, transfer, or mitigate the risk. Create a risk treatment plan (RTP) outlining

how each risk will be managed. Define and implement the processes and procedures re-quired for the ISMS. This involves establishing a risk management framework and defining roles and responsibilities for information security. Establish metrics to measure the effectiveness of in-formation security controls. Regularly monitor and review these metrics to ensure the ISMS is working as intended. Lastly it is important to conduct internal audits at planned intervals to ensure the ISMS conforms to planned arrangements and is effectively implemented and maintained. Management should also review the ISMS at planned intervals. Based on the results of internal audits, management reviews, or other relevant information, identify opportunities for improvement and make necessary adjustments to the ISMS.

9.4.5 ISO 27002 mitigation strategies

ISO 27002 offers detailed guidance on individual controls that can be used within the ISMS established by ISO 27001. Firstly, you need to understand the Controls. ISO 27002 provides a detailed set of controls that address specific areas of information security. These areas include security policy, organization of information security, human resource security, ac-cess control, cryptography, physical and environmental security, operations security, communications security, system acquisition, development and maintenance, supplier relationships, information security incident management, information security aspects of business continuity management, and compliance. Secondly you must select Appropriate Controls. Once you have identified the risks to your organization's information (as part of the ISO 27001 process), you can select appropriate controls from ISO 27002 to address these risks.

The next step is to implement these controls within your organization. This will often involve changes to business processes, IT systems, and physical layouts, as well as staff training. Controls are not set-and-forget. They need to be maintained, and their effectiveness needs to be reviewed on a regular basis. This is part of the ISO 27001 process of monitoring, reviewing, and improving the ISMS. Bear in mind, the ISO 27001 and ISO 27002 standards are designed

to work together. ISO 27001 lays out the requirements for an ISMS and ISO 27002 provides a set of best practice guidelines that can help fulfil those requirements. By following these standards, you can help ensure that your organization’s information is protected in a systematic and cost-effective.

9.4.6 BIMCO mitigation Strategies

The first phase is the Identification phase. Create an inventory of computer-based systems onboard to understand how to protect, detect, respond, and recover. Identify interdependencies across critical systems and assess risks. The second phase is the protection phase. The purpose of this phase is to design systems to support secure configuration, integration, and soft-ware maintenance. Limit the interoperability of systems to identified critical functions. Segment the OT and IT network infrastructure into zones. Restrict physical and logical access to OT systems. Minimize disruption to OT systems that could affect safety critical functions. The 3rd phase is the detection phase. This phase provide means for monitoring normal operations of OT systems based on self-diagnostics and network performance monitoring. The 4th phase is the respond phase which is a method for containing the impact of cyber incidents to the network zone of origin. This method aims at minimizing the extension of disruption to OT systems affecting safety critical functions. The 5th and last phase are the recovery phase. The purpose of this phase is to design equipment to support backup and restoration of OT systems in a timely manner. Implement network protection and detection systems by making use of firewalls to establish perimeter and internal security. Implement intrusion detection and prevention systems so the IT department can act accordingly. Deploy anti-virus software for systems with standard operating systems. Control wireless communication and access points. Implement data loss prevention and content filtering technologies. Apply advanced security measures such as virtual private networks (VPNs) and Security Information Event Monitoring (SIEM). Another important measure which is recommended by BIMCO is Ensuring physical access control. This can be done by Installing computer-based systems in locked or restricted areas. Implement physical security measures

to restrict access. Safeguard equipment and supporting utilities. Use physical security equipment such as surveillance cameras and electronic locks.

Lastly it is also important to Follow software assurance practices.
Design and develop software following structured procedures and standards. Implement logical security measures to prevent unauthorized modification of software. Validate and verify software according to software development standards. Consider backup and recovery of software and data. The reason behind choosing BIMCO Guidelines to find cybersecurity strategies is that it provides extensive guidelines specifically tailored to the maritime industry. The guidelines aim to improve the safety and security of seafarers, the environment, cargo, and ships by addressing the increasing cyber risks faced by the industry. It emphasizes the importance of managing cyber risks in a shipping context and provides recommendations on developing a proper cyber risk management strategy. The guidelines consider relevant national, international, and flag state regulations and guidelines, including the International Maritime Organization (IMO) resolution on Maritime Cyber Risk Management. By following these guidelines, maritime stakeholders can work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities.

9.4.7 DNV mitigation strategies

DNV highlights the importance of Increasing Investments in cyber security measures. It is recommended that maritime organizations invest more in cybersecurity to improve their security posture. This includes investing in technologies, training, and resources to ensure the protection of both IT and operational technology (OT) systems. DNV suggests that regulations and compliance requirements should be strengthened to ensure that maritime organizations meet cybersecurity standards. Compliance should be seen as a baseline, and organizations should strive for continuous improvement and proactively identify and manage new risks and weaknesses. Maritime organizations need to address supply chain vulnerabilities by auditing vendors' cybersecurity requirements and ensuring that suppliers have proper security measures in

place. This includes adhering to industry standards and implementing secure network architecture, access control, data protection, risk assessment, and incident response protocols. It is also important to mention the urgent need for better information sharing and collaboration within the industry. Maritime organizations should create forums and networks to facilitate open discussion, share information, and learn from each other's experiences. Transparency and information-sharing can help establish industry standards and best practices. Lastly It is crucial to provide effective cybersecurity training for employees at all levels within the organization. Training should focus on raising awareness about cybersecurity risks, teaching best practices, and ensuring the workforce understands their roles and responsibilities in maintaining a secure environment. Continuous training and reinforcement of cybersecurity practices are recommended.

10 GAPS AND CHALLENGES IN CURRENT CYBER SECURITY PRACTICES

Even though there is an increase in the concern and awareness of cyber security there is gaps and challenges that needs to be identified. These gaps are necessary to identify, to ensure that organizations are robust by adopting proactive cyber security measures and stay updated on the latest cybersecurity best practices. By addressing these gaps and challenges, organizations can enhance their cyber resilience and effectively protect their assets, data, and reputation. When carrying out maritime operations whether it is cargo operations, Dynamic Positioning operations, planned maintenance or maneuvering operations it is important that the challenges and gaps are identified to mitigate the risks involved in these tasks. Therefore, familiarization of the vessel is vital in the context of carrying out safe ship operations. Where are the backup systems? How do they work? Are the backup systems independent? How long do they work, if run by uninterrupted power supplies? What is the backup plan if all else fails? Who do we contact? How can we recognize the risks? These are

all questions that needs to be asked by the crew involved in ship operations in my opinion.

10.1 The gaps and challenges in current cyber security practices

Many employees, including seafarers, lack adequate awareness and training in cybersecurity best practices. This can lead to unintentional actions that expose the company and ship to cyber risks. The maritime industry relies on many legacy systems that are no longer supported or have outdated software and operating systems. These systems are more vulnerable to cyber threats as they may have known vulnerabilities that are not being addressed. Failure to regularly install software patches and updates is another risk that leaves systems exposed to known vulnerabilities that can be exploited by cybercriminals. This is something that can be done either via remote support from the onshore organization or via an external hard disk being send to the ship. Bearing in mind that both solutions have its own risks involved. Weak access controls and insufficient authentication measures can make it easier for unauthorized individuals to gain access to networks and systems. This includes default or easily guessable passwords and outdated access management practices. Many companies lack comprehensive contingency plans and procedures to respond effectively to cyber incidents. This can result in delays in identifying and containing threats, leading to increased damages. Companies often work with various third-party vendors and service providers who may have weak cybersecurity practices. If these vendors are not properly vetted and managed, they can introduce vulnerabilities and risks into the company's systems. It is therefore also very important that you as a company protect yourself against threats from 3rd party encounters. According to DNV there is a lack of consistent reporting and information-sharing on cyber incidents in the maritime industry. This hampers collective efforts to learn from past incidents and improve cybersecurity practices. This is also a claim that is supported by DNV.[28] Cyber threats are constantly evolving, with new attack vectors and techniques

[28] (Veritas, 2023) Page 35

emerging regularly. Keeping up with these threats and implementing appropriate countermeasures can be challenging for companies. The supply chains are at risk. Subverting the supply chain through compromised equipment, software, or supporting services poses risks to the company's systems and data. The lack of proper monitoring and detection measures makes it challenging to detect and respond to cyber incidents promptly. This limits the incident identification which can lead to further compromise of the cyber systems. Large challenges arise in aligning cybersecurity practices with national, international, and flag state regulations and guidelines. It is therefore vital that there is a higher focus on complying with the regulations in the industry. Overall, the industry needs to address these gaps and challenges to improve cybersecurity practices and mitigate the risks associated with cyber incidents. Both the BIMCO[29] and DNV[30] Reports highlight the similar challenges and gaps. DNV is however also giving recommendations which can be used to decrease and improve the gaps and challenges.

10.2 Recommendations from DNV

According to DNV, Maritime organizations should prioritize cybersecurity investment, both in IT and OT systems. Adequate funding is crucial for enhancing cyber resilience and adopting proactive measures to mitigate cyber risks. DNV finds that many organizations need to shift their focus from solely securing IT environments to ensuring the cybersecurity of OT systems. A holistic approach that includes integrating IT and OT security measures is necessary to protect critical infrastructure and ensure physical safety. DNV recognizes a need for enhancing the focus on training and awareness. DNV finds that organizations should provide comprehensive cybersecurity training to their employees at all levels, emphasizing the importance of cybersecurity practices and awareness of potential threats. Training programs should be regularly updated to address evolving cybersecurity risks. DNV also emphasizes a need

[29] (BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), , InterManager, International Association of Independent Tanker Owners (INTERTANKO) and many others, 2020) page 34-39
[30] (Veritas, 2023)

for Improving collaboration and Information Sharing. DNV believes that maritime organizations should foster a culture of collaboration and information sharing within the industry. Establishing forums, networks, and platforms to share best practices, lessons learned, and threat intelligence can help raise cybersecurity standards and maturity across the sector. DNV finds it important and necessary to stay ahead of regulations. This means that organizations should go beyond compliance with regulations and adopt proactive cybersecurity measures. They should continuously monitor and assess evolving cybersecurity threats, align their security practices with industry standards, and strive for continuous improvement. Address supply chain risks is also of importance to mitigate the risks of cyber incidents. Supply chain vulnerabilities requires rigorous vendor audits, adherence to cybersecurity requirements, and increased transparency. Maritime organizations should work closely with vendors to ensure the security of software and technology throughout the supply chain. According to DNV Efforts should be made to attract, develop, and retain skilled cybersecurity professionals. This can be achieved through partnerships with educational institutions, establishing cybersecurity training programs, and offering competitive incentives to attract talent to the maritime industry.[31]

11 STRATEGIES FOR ENHANCING CYBER SECURITY AWARENESS

Based on the different cybersecurity strategies in the various regulative frameworks and guidelines, I have assembled some strategies that can be implemented to enhance cyber security awareness among ship's crew. Firstly, it is important to develop an awareness program. Create a comprehensive cyber security awareness program specifically tailored to ship's crew. This program should include training sessions, workshops, and informative materials to educate crew members about cyber security risks and best practices. Just like the required drills onboard the ships, companies should conduct regular

[31] (Veritas, 2023) Page 42

training sessions. Schedule regular training sessions to ensure that crew members are updated on the latest cyber security threats and mitigation strategies. These sessions can cover topics such as identifying phishing emails, using strong passwords, and recognizing suspicious activities. It is also important to make sure crew members have easy access to relevant information and resources related to cyber security. This can include guidelines, checklists, and contact information for reporting cyber incidents or seeking assistance. For a shipping company to have success in cyber security awareness it is important to promote a cyber security culture. You can foster a culture of cyber security awareness by encouraging crew members to prioritize cyber security in their daily activities. Reinforce the importance of reporting any suspicious activities or potential cyber security incidents. It also important to Implement a reporting mechanism that allows crew members to report any cyber security incidents or concerns. This can include a dedicated email address or a confidential reporting system to ensure that incidents are promptly addressed. Collaboration with other shipping companies, industry associations, and regulatory bodies to share best practices and lessons learned in enhancing cyber security awareness is a strategy that could create a lot of long-term value. Participate in industry-wide initiatives to improve cyber security in the maritime sector. Another important strategy is to conduct regular assessments of crew members' cyber security awareness and knowledge. This can be done through quizzes, surveys, drills, or simulated phishing exercises to evaluate their understanding of cyber risks and identify areas for improvement. Another way of enhancing the awareness is to establish partnerships with IT experts or cybersecurity firms to provide additional expertise and guidance on enhancing cyber security awareness. These partners can offer specialized training sessions and provide ongoing support to address any emerging threats or challenges. It is also important that the industry stay updated on emerging threats. The shipping companies and the maritime industry must continuously monitor and stay updated on emerging cyber threats and vulnerabilities in the maritime industry. Regularly review industry reports, news, and alerts to ensure that awareness programs and training sessions are aligned with the latest trends and risks. For the awareness programs to have an effect it is important to continuously Improve the Awareness Program. Regularly evaluate the effectiveness of the

cyber security awareness program and make necessary improvements based on feedback and emerging threats. Seek input from crew members to ensure that the program meets their needs and addresses their concerns. By implementing these strategies, maritime organizations can enhance cyber security awareness among ship's crew and mitigate the risks associated with cyber threats in ship operations.

12 METHODOLOGY

12.1 Research Design

As mentioned above, training and awareness-raising is essential to prevent cyber-attacks. Awareness training is vital for the seafarers to be able to detect and eliminate cyber threats. However, the lack of current accessible data is limited and makes its valuation difficult. In this study, a questionnaire with clarifying questions regarding the level of cyber awareness among seafarers was distributed to seafarers of all ranks and ages. The aim was to focus on the current cyber security awareness among the seafarers and whether there is a need for further awareness training. To attain this knowledge, I needed quantitative data that was collected as primary data from a survey.

12.2 Data Collection

In this study, quantitative data collection method will be applied to gather relevant information from the relevant respondents. The primary data collection methods include a survey. A questionnaire was distributed to seafarers of all ages and ranks to assess their awareness of cybersecurity risks and measures. The survey will include questions on their knowledge of cyber threats and awareness regarding cyber security. The survey was running for 1 week from my Linkedin profile. The survey had 84 respondents when the survey finished. The survey was produced in Google Forms.

Relevant documents, such as industry guidelines and regulatory frameworks will be analyzed to collect additional data on cybersecurity practices and incidents in the maritime industry.

12.3 Data Analysis Strategy

12.3.1 Questionnaire Data.

The questionnaire aimed at creating an overview of the current cyber security awareness among seafarers and collected responses from 84 participants. The demographic breakdown of the respondents is as follows:

Gender: Most respondents were male (89.3%), while females accounted for 10.7%. A small percentage preferred not to disclose their gender.

Age: The largest age group among the respondents was 18-35 years (44%), followed by 36-55 years (38,1%) and 55+ years (17,9%).

Rank: The distribution of respondents based on rank was as follows: Ordinary Seaman (9,5%), Cadet (3,5%), Deck Rating/Able Seaman (14.3%), Junior Engineer (0,1%), Junior Officer (14.3%), and Senior Officer (42,9%) And Senior Engineer (15.5%).

When asked about their understanding of cyber security and its importance, most respondents (96.4%) answered positively, indicating a good level of awareness among seafarers.

Regarding the awareness of cyber security policies and procedures in their companies, a high percentage (92.9%) of respondents claimed to be aware, suggesting that companies prioritize cyber security measures.

78,6% indicated that they have received training in cybersecurity awareness. a large percentage of respondents (17.9%) reported having received no training or education on cyber security.

The questionnaire also assessed the participants' familiarity with various cyber threats. The results showed that the most recognized threat was Malware, with 91.7% of respondents identifying it. Other well-recognized threats included Phishing (89.3%), Ransomware (70.2%), and Social Engineering 25% and Denial of Service (21.4%).

When asked about the ability to identify phishing emails or malicious websites a high percentage 82,1% indicated having the knowledge to identify phishing mails and malicious websites a low percentage (13.1%) of respondents expressed a lack of confidence in their skills.

Regarding actions to take in the event of a suspected cyber security incident, 88.1 % knew who to contact in case of a cyber security incident.

A significant majority of respondents (97.6%) acknowledged that portable devices, such as USB-drives and smartphones, can be potential sources of cyber threats.

Concerning personal device usage on the ship's network, 44% of respondents admitted to connecting their personal devices sometimes, while 51,2% stated that they did not connect at all.

Awareness of the risks of sharing sensitive information on an unsecure network was high, with 92,9% of respondents being aware of this potential security breach.

When asked about identifying unusual activity or potential signs of security breaches, 31% of respondents expressed that they were not sure how to do so, while a large amount (60.7%) expressed certainty.

A significant percentage (64.3%) of respondents reported having never noticed unusual activity or potential signs of cyber security breaches on the ship's network.

When asked about knowing the appropriate actions to take in the event of compromised IT, navigation, communication, or operation systems, 72,6% of respondents felt confident in their knowledge.

Finally, when asked if their companies could do more to raise cyber security awareness, 27.4% of respondents answered no, while 22.6% were uncertain, and most 50% answered yes.[32]

12.4 Evaluation and justification

The reason for choosing quantitative method for this thesis is to obtain numerical data and perform a descriptive analysis to objectively assess the research objectives. This approach can provide a more systematic and structured analysis, allowing for generalization and the identification of patterns or trends in the data. By using quantitative method, I can use statistical methods to analyse and interpret the data collected, enabling the identification of relationships between variables and the assessment of the significance of these relationships. This can lead to new knowledge and understanding by providing empirical evidence to support or refute the theories or hypotheses of my thesis project.

The strength of quantitative method includes various things. For once objectivity is important. Quantitative method relies on numerical data, which can be objectively measured and analysed. Generalizability is another important matter in gaining good reliable quantitative data. With a larger sample size, quantitative data can provide more representative results that can be generalized to the larger population. Replicability is also very important when collecting quantitative data. The use of standardized measurement tools and statistical tests allows for the replication of the study by other researchers, ensuring the

[32] (Sørensen, 2023)

reliability of the findings. However, there are also limitations and weaknesses of quantitative analysis which includes the potential lack of contextual information. Quantitative methods may focus on numerical data and may not capture the rich contextual information that qualitative methods can provide. Reductionism is another important matter. Quantitative analysis often requires simplification and reduction of complex phenomena into measurable variables, potentially oversimplifying the complexity of real-world situations. And lastly the potential for bias exist when conducting quantitative data methods. The data collection and analysis process in quantitative research can be influenced by researcher bias and subjectivity. It is important to consider these limitations and strengths when choosing quantitative methods for a research study and to carefully design the research to address the research objectives and minimize potential weaknesses.

12.5 Ethical Considerations

Ethical Considerations: Throughout the research process, ethical considerations will be considered, and appropriate measures will be implemented to ensure the privacy, confidentiality, and informed consent of the participants. The study will comply with ethical guidelines and obtain ethical approval from the relevant authorities. By employing the quantitative methodology, this study aims to provide a comprehensive and rigorous analysis of cybersecurity in the shipping industry. The combination of literature review, data collection, and analysis will enable a thorough exploration of the research topic and contribute to the existing knowledge in the field.

13 ANALYSIS

13.1 Presentation of data and analysis strategy.

The data was obtained through a framework consisting of a variety of literature reviews and a quantitative survey with seafarers in the shipping industry to either contradict or prove that my problem statement is valid. The findings are analysed to identify key insights and trends related to cyber security awareness. The data collected revealed several key findings regarding cyber security awareness strategies, cyber security risks in ship operations, methods for identifying and assessing these risks, and strategies for mitigating them.

13.2 Analysis of Data

13.2.1 “The Human Factor” and the vulnerabilities in human cyber interaction.

In the literature review vulnerabilities in cyber security is discussed without considering thoroughly that human beings can also be a part of the vulnerabilities when discussing cybersecurity due to several reasons. Firstly, humans can unintentionally introduce vulnerabilities through their actions or lack of awareness. For example, employees may click on malicious links or download infected files, unknowingly granting access to cyber attackers. Additionally, weak passwords or password reuse can make it easier for attackers to gain unauthorized access to systems this is also backed up by DNV.
Furthermore, social engineering techniques, such as phishing, rely on human manipulation to trick individuals into revealing sensitive information or performing actions that can compromise security. Cyber attackers often exploit human psychology, trust, and social engineering tactics to deceive individuals and gain access to systems. Moreover, human errors and lack of proper training can contribute to cybersecurity vulnerabilities. Employees who are not properly trained in cybersecurity best practices may unknowingly engage in unsafe behaviour, such as sharing sensitive information or falling for phishing scams. Overall, addressing human vulnerabilities is crucial in cybersecurity, as

individuals play an important role in safeguarding systems and data. By promoting cybersecurity awareness, providing comprehensive training, and implementing strong security protocols, organizations can mitigate human-based vulnerabilities and enhance their overall cybersecurity posture.

13.2.2 How the shipping companies can make use of the BIMCO guidelines.

Shipping companies can use these guidelines as a foundation for enhancing cyber security awareness among seafarers. Incorporate cyber security training in crew training programs: Shipping companies can include cyber security training modules in their regular crew training programs. These modules should cover topics such as identifying cyber threats, safe online practices, recognizing phishing emails, and reporting suspicious activities. By educating seafarers about potential cyber risks and providing them with the knowledge and skills to mitigate those risks, shipping companies can foster a cyber security-aware culture onboard. By conducting regular cyber security drills and exercises Like safety drills, shipping companies should organize regular cyber security drills and exercises for seafarers. These drills can simulate various cyber security scenarios, such as phishing attacks or malware infections, and test the crew's response and awareness. Through hands-on practice, seafarers can learn how to effectively respond to cyber incidents and take necessary actions to protect themselves and the ship's systems. it is also important to encourage the seafarers to report any cyber security incidents or suspicious activities they encounter onboard. Establish a clear reporting process and assure seafarers that their concerns will be taken seriously and addressed appropriately. This promotes a proactive approach to cyber security and helps identify vulnerabilities or emerging threats more quickly. The shipping companies should make relevant cyber security resources, guidelines, and best practices easily accessible to seafarers. This can include providing electronic copies of the guidelines on cyber security onboard ships, along with additional resources from reputable sources such as industry associations or government agencies. By giving seafarers access to such information, they can continually update their knowledge about cyber security and implement best

practices in their daily operations. Another important aspect is to foster a culture of open communication between the crew and management regarding cyber security concerns. Establish channels for seafarers to raise any cyber security-related questions, provide feedback, or report potential vulnerabilities. This creates a collaborative environment where seafarers feel comfortable discussing cyber security issues and actively participating in the company's cyber risk management efforts. It is of vital importance that shipping companies and the shipping industry continuously review and update their cyber security policies and procedures to stay aligned with evolving cyber threats and industry best practices. Communicate any changes or updates to seafarers and ensure they understand and follow the revised guidelines. Regularly reviewing and updating policies not only enhances cyber security awareness but also demonstrates the company's commitment to protecting its assets and data. By implementing these measures, shipping companies can raise cyber security awareness among seafarers and empower them to be proactive in mitigating cyber risks onboard ships. This proactive approach to cyber security helps create a safer and more resilient maritime industry.

13.2.3 How the shipping companies can make use of the existing regulatory frameworks

The companies must start by thoroughly studying the regulatory framework, such as the guidelines provided by the International Maritime Organization (IMO) and the International Association of Classification Societies (IACS). It is vital for shipping industry to understand the requirements and recommendations outlined in these frameworks, including the need for cyber risk management and the importance of incorporating cyber security into safety management systems. Firstly evaluate the company's current cyber security practices and compare them to the requirements set by the regulatory framework. Identify any gaps or areas for improvement in terms of cyber security awareness, training programs, incident response planning, and risk management. Secondly it is important to develop and implement a cyber security management plan that aligns with the company's safety management system. Incorporate cyber security policies, procedures, and controls into existing safety

management processes to ensure that cyber security awareness becomes an integral part of the company's operations. Here it is relevant to implement ISO standards as a part of the cyber security systems in the company. The ISO standards provide standards, practises, and audits, which will enhance the cyber security awareness and robustness in the entire organisation. For people to understand the importance of cyber security it is vital to develop comprehensive training and awareness programs for all employees, including seafarers and shore-based personnel. Train them on the importance of cyber security, common threats, and best practices for preventing and responding to cyber incidents. Make the training programs interactive and engaging to ensure maximum effectiveness. Actively participating in collaboration initiatives and information-sharing platforms within the maritime industry. Share experiences, lessons learned, and best practices related to cyber security. Learn from others' experiences and provide insights to help improve the overall cyber security awareness and resilience of the industry. DNV also recommends this as an active way of enhancing the awareness and robustness on long term. It is important for the shipping companies to establish processes for continuous monitoring of cyber security practices and performance. Regularly assess the effectiveness of training programs, incident response plans, and risk management strategies. Collect feedback from employees and stakeholders to identify areas for improvement and make necessary updates to enhance cyber security awareness. By utilizing the regulatory framework, shipping companies can enhance their cyber security awareness efforts. This will help them to better protect their systems, data, and personnel from cyber threats and ensure the continued safe and secure operations of their ships.

13.2.4 The limitations in the guidelines and regulatory framework

While using regulatory frameworks can greatly enhance a shipping company's cyber security awareness and practices, there are still several potential limitations and challenges to consider. It can be dangerous to have a “One-size-fits-all Approach” regulatory frameworks often provide universal standards that may not account for the unique needs and circumstances of every shipping

company. For example, a small shipping firm may lack the resources to implement the same cyber security measures as a large multinational corporation. The framework may not provide enough flexibility or guidance for these different situations. While regulatory frameworks are designed to provide guidelines, they may not be specific or detailed enough to be directly implemented. This could lead to different interpretations and applications of the guidelines, potentially resulting in inconsistent levels of cyber security awareness and protection across the industry. Given the rapid pace of technological change and evolving cyber threats, regulatory frameworks may become outdated quickly. The process to update these frameworks can be slow and bureaucratic, which could leave shipping companies vulnerable to new types of cyber-attacks that are not addressed in the current guidelines. For the industry and companies to ensure compliance with the regulatory framework can be challenging. Without effective mechanisms to monitor and enforce compliance, some companies may neglect or fail to fully implement the recommended cyber security measures. Furthermore, the penalties for non-compliance may not be severe enough to deter negligent behaviour. It is vital to understand that implementing the recommendations of a regulatory framework can be resource intensive. This includes the costs of developing and maintaining cyber security infrastructure, training staff, and conducting regular audits and assessments. Some companies, particularly smaller ones, may struggle to afford these investments. There's a risk that companies might focus too much on ticking boxes to meet the regulatory requirements, rather than building a robust and proactive cyber security culture. Compliance does not necessarily equate to security, and a company can meet all the regulatory requirements yet still be vulnerable to cyber-attacks. The lack of global uniformity is a cause for concern. While organizations like IMO offer guidelines, the actual regulation and enforcement can vary significantly by country. This inconsistency can make it difficult for multinational shipping companies to ensure they are compliant with all relevant cyber security regulations. Despite these limitations, a regulatory framework still provides an important foundation for enhancing cyber security in the shipping industry. Companies should complement these guidelines with their own proactive measures tailored to their specific needs and circumstances.

13.2.5 The NotPetya incident and its importance

The NotPetya incident serves as a significant example of the importance of enhancing cyber security awareness among seafarers in the maritime industry. The incident, which occurred in June 2017, was a global ransomware attack that had severe consequences for various industries, including shipping and logistics. During the NotPetya attack, Maersk, a major shipping company, was one of the most severely affected organizations. The attack infected and shut down Maersk's computer systems across 130 countries, making it impossible for the company to manage its port and terminal operations. As a result, Maersk experienced significant disruptions in its shipping operations, with delays in processing orders and handling cargo. The impact on Maersk's financials was substantial, with estimated costs ranging from $250 million to $300 million. The company had to revert to manual processes, causing significant operational delays and financial losses. Maersk also faced reputational damage as customers experienced delays and inconveniences due to the attack. This incident highlights the vulnerability of the shipping industry to cyber threats and the need for enhanced cyber security awareness among seafarers. Seafarers play a crucial role in the operations of ships and are often the first line of defence against cyber-attacks. By being aware of cyber security risks, seafarers can be more vigilant in identifying and reporting potential threats or suspicious activities. Enhancing cyber security awareness among seafarers can help prevent incidents like NotPetya by educating them on best practices for cyber hygiene, such as recognizing phishing emails, managing passwords securely, and reporting any unusual or suspicious activities. Seafarers need to understand the potential consequences of cyber-attacks on ship operations, safety, and the environment, as well as the financial impact on their organizations. Training and awareness programs should be implemented to educate seafarers about the latest cyber security threats, attack techniques, and preventive measures. It is essential to provide regular updates and refreshers on cyber security practices, as the threat landscape is constantly evolving. This is also perfectly aligned with the strategies of DNV who recommends further awareness training as a part of improving the cyber security robustness. Furthermore, cyber security awareness should extend beyond seafarers to

include all personnel involved in ship operations, including shore-based staff, IT teams, and management. Collaboration and information sharing between the different stakeholders in the industry can help raise awareness and promote effective cyber risk management. This requires an interest in increasing the investments on cyber security measures which is also highlighted by DNV as an important factor for enhancing the level of cyber security in the industry. In conclusion, the NotPetya incident serves as a reminder of the potential consequences of cyber-attacks on the maritime industry. Enhancing cyber security awareness among seafarers is paramount in protecting ship operations, personnel, and critical systems from cyber threats. By fostering a culture of cyber security awareness and providing proper training, the maritime industry can better defend against cyber-attacks and mitigate the risks associated with them.

13.2.6 Analysing current gaps and challenges in the shipping industry

One of the significant challenges in cyber security is the lack of awareness and training among employees at all levels. Many individuals, including seafarers, lack the necessary knowledge and understanding of cyber security best practices. This can lead to unintentional actions that expose the company and ships to cyber risks. To address this gap, organizations need to prioritize cyber security training and awareness programs that cover topics such as recognizing phishing emails, password hygiene, and reporting suspicious activities. Further investments are also supported by DNV and its perfectly aligned with the results in the quantitative survey analysis. The maritime industry relies on many legacy systems that are no longer supported or have outdated software and operating systems. These systems are more vulnerable to cyber threats as they may have known vulnerabilities that are not being addressed. Organizations need to invest in upgrading or replacing these legacy systems to ensure they are protected from cyber-attacks. Another challenge is the failure to regularly install software patches and updates. This leaves systems exposed to known vulnerabilities that can be exploited by cyber criminals. Organizations need to establish robust patch management practices to ensure their systems

are up to date and protected from the latest threats. Another large vulnerability is weak access controls and insufficient authentication measures make it easier for unauthorized individuals to gain access to networks and systems. Organizations need to implement strong access controls, including two-factor authentication and the principle of least privilege, to limit access to critical systems and data. The lack of contingency plans is a cause for concern. Many companies lack comprehensive contingency plans and procedures to respond effectively to cyber incidents. This can result in delays in identifying and containing threats, leading to increased damages. Organizations need to develop and regularly test their incident response plans to ensure they can respond promptly and effectively to cyber security incidents. Working with third-party vendors and service providers introduces additional cyber security risks. If these vendors do not have robust cyber security practices, they can introduce vulnerabilities into the company's systems. Organizations need to rigorously vet and manage their third-party relationships to ensure the security of their data and systems. The maritime industry lacks consistent reporting and information sharing on cyber incidents. This hampers collective efforts to learn from past incidents and improve cyber security practices. Organizations need to encourage information sharing and collaboration within the industry to raise overall cyber security standards. It is important for the industry that they recognize that cyber threats are constantly evolving, with new attack vectors and techniques emerging regularly. Organizations need to continuously monitor the threat landscape and update their cyber security measures accordingly to stay one step ahead of potential attackers. Supply chain vulnerabilities is important to recognize to keep your organization safe. Subverting the supply chain through compromised equipment, software, or supporting services poses risks to the company's systems and data. Organizations need to conduct rigorous vendor audits, enforce cyber security requirements, and increase transparency in the supply chain to mitigate these risks. Many organizations lack robust monitoring and detection measures, making it challenging to detect and respond to cyber incidents promptly. Organizations need to invest in robust threat detection systems and establish incident response teams that can effectively respond to cyber security incidents. In conclusion, addressing the gaps and challenges in cyber security requires a holistic approach that

involves awareness and training, upgrading legacy systems, implementing robust access controls, developing comprehensive contingency plans, managing third-party risks, promoting information sharing, staying ahead of the evolving threat landscape, mitigating supply chain vulnerabilities, and enhancing incident detection and response capabilities. By addressing these challenges, organizations can enhance their cyber security posture and mitigate the risks associated with cyber security incidents.

13.2.7 Analysis of awareness strategies.

Firstly, the development an awareness program is a crucial step as it forms the foundation for cyber security education among the crew. However, the effective-ness of the program would depend on the content and how well it is tailored to the maritime industry and the crew's specific needs. It should be developed in a language and format that is easy to understand for all crew members, regardless of their technical proficiency. Regular training is also vital to keep the crew updated and vigilant. However, the challenge lies in scheduling these sessions in a way that doesn't hamper the crew's primary responsibilities. Using engaging and interactive training methods can improve participation and retention of information. It is also very important to provide information and resources. While this strategy is important, the effectiveness would depend on how accessible and user-friendly these re-sources are. Moreover, the crew should be encouraged to use these re-sources regularly. Promoting a Cyber Security Culture in the industry is vital for obtaining success with this strategy. This is an effective long-term strategy but might face resistance initially as it requires a change in behaviour and attitude. Leadership commitment is crucial in promoting a cyber security culture. Reporting Mechanisms is another important tool. The success of this strategy depends on how safe the crew members feel about reporting incidents without the fear of repercussions. It also depends on how efficiently the reported incidents are handled. Collaboration with Industry stakeholders can provide a lot of value for the entire industry. This strategy can bring in a wealth of knowledge and experience, but the challenge lies in finding the right partners and maintaining an active

collaboration. Confidentiality is another factor to consider when sharing information with outside entities. It is important to conduct regular assessments. This strategy is effective in measuring the success of the awareness programs. However, it needs to be done in a non-intrusive way and the results should be used to improve the programs rather than punish the crew members. By developing partnerships with IT experts this strategy can bring in the needed expertise, but it may also involve additional costs. Choosing the right partners who understand the unique requirements of the maritime industry is also crucial. It is an ongoing requirement and can be resource intensive to stay updated on emerging threats. However, it's necessary to ensure the training and awareness programs always remain relevant and up to date. It is also of vital importance to continuously Improve the awareness program. This strategy is important for the long-term success of the program. However, obtaining feedback from the crew members and implementing changes based on that feedback can be challenging and time-consuming. Overall, while these strategies can greatly enhance cyber security aware-ness, however their success largely depends on the commitment of the leadership, the willingness of the crew to participate, and the availability of resources. Regular evaluation and improvement of these strategies are also required to ensure they remain effective in the face of evolving cyber threats.

13.2.8 analysis of the mitigation strategies and guidelines

13.2.9 IACS Strategy

The recommendation emphasizes the importance of conducting a thorough risk assessment to identify potential cyber risks and vulnerabilities. This as-assessment should consider the requirements of international conventions, classification societies, and national authorities. The recommendation addresses technical design, construction, and testing aspects. It suggests incorporating cyber resilience measures into the design and construction of computer-based systems on board ships. This includes implementing secure operation measures and protection against unauthorized access, misuse,

modification, destruction, or improper disclosure of in-formation. The recommendation also highlights the need for testing and verification of cyber resilience measures. This involves conducting tests to ensure the effectiveness of security controls and to verify that the systems can withstand cyber incidents. It also emphasizes the importance of regular maintenance and updates to address emerging threats. While the recommendation primarily focuses on technical aspects, it acknowledges the importance of operational aspects and management items. It suggests that owners and operators should assume responsibility for operational aspects and follow guidance provided in Annex A, which includes contingency planning and response processes in the event of a cyber incident. The recommendation emphasizes the need for compliance with relevant guidelines, standards, and regulations. It encourages continuously improvement by staying updated on emerging threats, conducting regular risk as-assessments, and implementing necessary measures to enhance cyber resilience. Overall, the recommendation provides a comprehensive approach to coping with cyber incidents on ships, covering risk assessment, design, and construction, testing and verification, operational aspects, and compliance and continuous improvement.

13.2.10 BIMCO strategy

During the Identification phase it is important to create an inventory of computer-based systems onboard is fundamental for understanding the extent and nature of the cyber infrastructure. It provides the basis for risk assessment, security planning, and incident response. The extent of this task's effectiveness will depend on its thoroughness and the accuracy of the inventory. Identifying interdependencies across critical systems and assessing risks: This is crucial in understanding the potential cascading effects of system failures or cyberattacks. It allows for prioritization of systems for protective measures. Effectiveness will depend on the quality of the risk assessment and the understanding of system interdependencies. The purpose of the protection phase is to design systems for secure configuration, integration, and software maintenance. This is a proactive approach that seeks to minimize vulnerabilities from

the onset. It is highly effective when done right, though it requires considerable expertise and effort. It is Limiting interoperability of systems to critical functions; this reduces potential points of failure or attack and is thus an effective strategy. However, it may limit system functionality and flexibility. Segmenting the OT and IT network infrastructure is important in this phase. This is an effective strategy for limiting the spread of potential cyber threats. However, the effectiveness will depend on the proper implementation of access controls between zones. During this phase it is also important to restrict physical and logical access to OT systems. This is effective in reducing the risk of unauthorized access but requires rigorous controls and vigilance. Lastly Minimizing disruptions to OT systems affecting safety. This strategy is crucial for maintaining safety but depends on effective system design and resilience measures. The detection phase purpose is to provide means for monitoring normal operations. This is a key strategy for early detection of anomalies or attacks. The effectiveness will depend on the quality of the monitoring tools and the ability to correctly interpret the data. The purpose of the respond phase is to Contain the impact of cyber incidents: An effective strategy that aims to minimize the damage. Success depends on rapid detection, effective incident response plans, and well-trained personnel. Minimizing the extension of disruption to OT systems is vital for maintaining operations and safety but requires the ability to quickly isolate and address issues. The purpose of the recovery phase is to design equipment for backup and restoration. This is a crucial strategy for ensuring continuity of operations. The effectiveness will depend on the quality of backup systems and the speed of restoration. During this phase it is vital to Implement network protection and detection systems by using firewalls, intrusion detection and prevention systems, anti-virus software, wireless communication control, data loss prevention, content filtering technologies and VPNs. These are all standard and effective cybersecurity measures. Their effectiveness will depend on correct configuration, regular updates, and correct usage. Another important aspect is to ensure physical access control. This can be done by Implementing computer-based systems in locked areas, restricting physical access, safeguarding equipment, and using physical security equipment: These strategies are effective in preventing unauthorized access, theft, and physical tampering. Their success depends on rigorous implementation

and monitoring. Lastly it is very important in this phase to follow software assurance practices. Structured design and development, logical security measures, software validation, and backup and recovery planning: These strategies are effective in ensuring the reliability and integrity of software. Their effectiveness will depend on the thoroughness of implementation and adherence to standards.

13.2.11 ISO 27001 and ISO 27002 mitigation strategies

ISO 27001 and ISO 27002 recommend implementing network segmentation as a means of separating different systems and restricting access between them. This strategy helps to minimize the potential impact of a cyber-attack by containing any potential breaches within specific segments of the network. Network segmentation is a widely recognized best practice in cyber security. It allows for granular control of network traffic and limits the lateral movement of cyber threats. By implementing network segmentation, organizations can better protect critical systems and sensitive data by compartmentalizing them from less critical areas of the network. The standards emphasize the need for deploying firewalls at the network perimeter and between network segments. Firewalls act as barriers between trusted internal networks and untrusted external networks, filtering and monitoring incoming and outgoing network traffic. Firewalls are an essential component of any robust cyber security strategy. They provide a first line of defence by inspecting network traffic and blocking unauthorized access attempts. By enforcing access policies and monitoring network activity, firewalls help to protect against unauthorized access and potential malware infections. ISO 27001 and ISO 27002 stress the im-portance of defining and enforcing access control policies and authorization mechanisms for human users, software processes, and devices. This includes measures such as multi-factor authentication, explicit access request approval, and session termination. Access control and authorization are fundamental elements of cyber security. By implementing strong access controls, organizations can ensure that only authorized individuals and systems can access sensitive resources. Multi-factor authentication adds an extra layer of

security, making it much more difficult for attackers to gain unauthorized access. The standards emphasize the im-portance of providing security updates to users, documenting product security updates, and regular maintenance activities. This includes keeping soft-ware and systems up to date with the latest patches, updates, and bug fixes. Regularly updating software and systems is critical to maintaining a strong security posture. Updates often address newly discovered vulnerabilities and provide patches to protect against known exploits. By staying current with security updates, organizations can mitigate the risk of cyber-attacks targeting known vulnerabilities. Overall, the cyber security mitigation strategies provided by ISO 27001 and ISO 27002 are comprehensive and aligned with industry best practices. They address critical areas of cyber security such as network segregation, access control, and regular maintenance. Implementing these strategies can significantly enhance an organization's cyber security posture and protect against a wide range of cyber threats.

13.2.12 DNV Strategies

Investing in cybersecurity is a strategy with potentially high return-on-investment due to the high cost of cyber-attacks and data breaches. A successful attack can result in significant financial loss, damage to reputation, and regulatory penalties. Therefore, investing in cybersecurity can be seen as a form of risk management. However, the challenge lies in determining where to allocate resources for maximum impact. This requires a deep understanding of the organization's specific risk profile, which can be complex in maritime operations due to the interconnection of IT and OT systems. Additionally, the rapidly evolving nature of cyber threats means that investments must be ongoing and adaptable. Organizations should also ensure that investments are not solely focused on technology, but also include people and processes, as these are often the weakest links in cybersecurity. Strengthening regulations and compliance requirements can help raise the minimum cybersecurity standards across the maritime sector. This can be particularly effective in industries where there is a wide disparity in the maturity of cybersecurity practices.

However, compliance does not guarantee security. Regulations often lag the evolving threat landscape and may not cover all potential risks. Additionally, focusing too much on compliance can lead organizations to adopt a checkbox mentality, where the goal becomes meeting regulatory requirements rather than achieving robust security. Therefore, while compliance is necessary, it should be treated as a baseline rather than the end goal. Given the interconnected nature of supply chains, a vulnerability in one organization can pose a risk to all. Therefore, securing the supply chain is a crucial strategy. This strategy, however, can be challenging to implement due to the complexity and opacity of supply chains. It requires deep collaboration and trust between organizations, as well as robust auditing and monitoring processes. Vendor management can also be resource-intensive, and smaller organizations may struggle to enforce their security requirements on larger suppliers. Information sharing can significantly improve collective defence by allowing organizations to learn from each other's experiences and respond to threats more quickly. It can also help establish industry standards and best practices. The challenge with this strategy is that it requires a high level of trust and openness, which may not come naturally in competitive industries. Organizations may also be reluctant to share information about breaches due to fear of reputational damage or legal repercussions. Therefore, creating a safe and confidential environment for information sharing is key. Employees are often the first line of defence against cyber-attacks, so training and awareness are crucial. A workforce that understands their roles and responsibilities in maintaining a secure environment can significantly reduce the risk of human errors leading to security incidents. However, training must be ongoing and engaging to be effective. Cybersecurity is a rapidly evolving field, and what was relevant a year ago may not be today. Training must also be tailored to different roles within the organization, as not everyone needs the same level of technical knowledge. Finally, while training can reduce the risk of human error, it cannot eliminate it completely. Therefore, it should be complemented with other strategies, such as strong access controls and incident response plans. In conclusion, all these strategies have their strengths and challenges. A comprehensive and effective cybersecurity program will likely involve a combination of these strategies, tailored to the specific needs and risk profile of the organization. When combining

the IACS, BIMCO, ISO and DNV strategies and guidelines they have similarities which can be useful in mitigating cybersecurity risks. The IACS recommendations lay a foundation for constructing cyber resilient vessels whereas BIMCO can be useful for an even further extensive mitigation strategy which can be used onboard, ISO supports the foundation and develop further mitigation strategies through audits and continuous development and lastly DNV is providing a current cybersecurity status while at the same time recommending strategies for the industry of shipping. All these strategies put together can provide a solid foundation for mitigating cybersecurity risks and enhancing the cybersecurity awareness in the industry.

The one thing that the legal frameworks have in common is that there is a high focus on mitigating the cyber risks through various IT and OT systems, risk assessment, segregation, and various other mitigation strategies. There is still not the widely needed cyber security awareness strategies for the seafarers. There are suggestions for strategies, but the quantitative data analysis indicate that there are still large gaps in this mitigation strategy.

13.2.13 Quantitative data analysis

Gender: Most respondents were male (89.3%), indicating that there is a gender imbalance among seafarers with regards to cyber security awareness. Efforts should be made to encourage more female participation and awareness in this field.

Age: The highest percentage of respondents belonged to the 18-35 years age group (44%), suggesting that younger seafarers may have a better understanding of cyber security, possibly due to more experience and exposure to technology. Efforts should be made to raise awareness among the older age groups, as they may have a higher risk of encountering cyber threats due to the lack of technological exposure in general.

Rank: The distribution of respondents based on rank shows that Senior Officers form the largest group (42.9%), followed by Senior Engineers (15.5%). It is essential to ensure that cyber security training and education reach all ranks, as each role may have different vulnerabilities and responsibilities regarding cyber security. The training must be simple to understand so everyone who is exposed to Information Technology understands the potential risks.

Understanding of Cyber Security: An overwhelmingly high percentage of respondents (96.4%) reported understanding what cyber security is and why it is important. This indicates a generally high level of awareness among seafarers, which is a positive finding. However, bearing in mind that even though the seafarers recognize its importance it does not necessarily imply that the seafarers know what to look for in cyber security risks. The analysis of the data will indicate that there is still a relatively large gap in awareness training.

Awareness of Policies and Procedures: Most respondents (92.9%) claimed to be aware of the cyber security policies and procedures in their companies. This suggests that companies are taking measures to communicate and enforce cyber security protocols, which is crucial for overall cyber resilience. This is positive and it indicates that procedures are easily accessible for the seafarers. It is however disturbing that even though policies and procedures are easily accessible they are however largely ignored when considering the risks involved in connecting private devices to the on-board IT systems. This is a cause for concern.

Training and Education: The questionnaire revealed that a relatively large percentage of respondents (78.6%) have received training or education on cyber security. This finding demonstrates a good overall focus on training in cyber security awareness programs for seafarers but there is room for improvement. A large percentage of respondents (17.9%) reported having received no training or education on cyber security, indicating a large gap in educational initiatives for seafarers. This Is a cause for concern and something that underlines my thesis regarding the necessity for more awareness training. Companies

and relevant authorities should keep prioritizing and providing regular training and education to enhance seafarers' knowledge and skills in this area.

Recognition of Cyber Threats: The respondents showed a good understanding of various cyber threats, with high recognition rates for Denial of Service (91.7%), Phishing (89.3%), and Malware (70.2%). However, there is room for improvement in recognizing threats like Social Engineering and Ransomware, as the recognition percentages were relatively lower. Future awareness training will have to involve a wide cyber security perspective that informs about all potential cyber threats in a simple and informative way.

Identification of Phishing and Malicious Websites: The questionnaire revealed that a large percentage of respondents (82.1%) feel confident in identifying phishing emails or malicious websites. This highlights a good overall level of awareness. However, with 17,9 percent either feeling unaware or not sure this indicates a need for further cyber security awareness training for the seafarers.

Preparedness for Cyber Security Incidents: The findings indicate that there is good level of preparedness among seafarers in terms of knowing who to contact and what actions to take in the event of a suspected cyber security incident (88,1%) answered yes. The rest of the responds either did not know or was not sure. Continuous efforts should be made to provide clear protocols and guidelines to seafarers to ensure appropriate responses to such incidents. No one must be in doubt of who to contact in case of emergencies.

Awareness of Portable Devices as Cyber Threat Sources: A significant majority of respondents (97.6%) acknowledged that portable devices can be potential sources of cyber threats. This finding indicates a high level of awareness regarding the risks associated with the use of personal devices on ships. But the fact that 44% still connect their personal devices on the ships network indicates they the respondents do not actually recognize the risks involved. This is a cause for concern.

Personal Device Usage on Ship's Network: The questionnaire revealed that a large amount of the respondents (44%) admitted to connecting their personal devices (such as personal phones) to the ship's network. This practice can increase the risk of security breaches, and it is essential to educate seafarers about the potential risks and best practices for secure device usage. When you are aware of the risks and continue what you are doing then we have to question you and your actual understanding of the risks involved.

44% is many respondents defying the risks, thereby indicating that they are aware of the risks of connecting personal devices, but they connect their personal devices anyways. So many persons defying the risks shows that the actual awareness and knowledge of the risks are limited. Thereby I will also question the validity of most respondents (97.6%) acknowledged that portable devices can be potential sources of cyber threats. I do not believe the respondents are aware of the actual risks when 44% defy the risks.

Sharing sensitive information on an unsecure network:
92,9% indicate that they understand sharing sensitive information in an unsecure network can be a security risk.

Identification of Unusual Activity or Security Breaches: The results showed that 31% of respondents claimed to be unsure how to identify unusual activity or potential signs of security breaches, while most respondents (60.7%) expressed they were aware. This finding highlights a need for training programs to enhance seafarers' skills in detecting and reporting security incidents. This is aligned with my thesis theory that there is a need for further awareness training.

Noticing Unusual Activity on Ship's Network: A significant percentage (64.3%) of respondents reported having never noticed unusual activity or potential signs of cyber security breaches on the ship's network. This indicates that seafarers are not vigilant or observant, which is critical for maintaining cyber security onboard ships. This large number indicates a clear need for further training in unusual cyber activities. I will therefore also question whether the 60.7%

of respondents are able to identify unusual activities in general. There is a clear gap between what respondents think they know and what the numbers are saying.

Actions to Take in Case of Compromised Systems: The findings reveal that with 72,6% indication that they are aware of what actions to take there is still a lack of knowledge among seafarers regarding the actions to take if ship's IT, navigation, communication, or operation systems show signs of compromise. However, 27,4% is lacking knowledge in how to take proper action and I find this quite alarming. Efforts should be made to ensure that seafarers are equipped with the necessary knowledge and guidance to respond effectively to such situations.

Company's Role in Raising Cyber Security Awareness: A significant percentage of respondents (50%) feel that their companies could do more to raise cyber security awareness. This finding suggests that companies should review and enhance their awareness initiatives to address seafarers' concerns and increase their overall cyber resilience. It also underlines my thesis theory that there is a large gap in cyber security awareness training for seafarers. [33]

13.3 Discussion of Results

The analysis of the results and trends identified in the data reveals the complex nature of cyber security in the shipping industry. The discussion of the results focuses on the implications of these findings and their significance for enhancing cyber security awareness and implementing effective measures in the shipping industry. The results highlight the critical importance of raising cyber security awareness among seafarers. The analysis emphasizes the need for comprehensive training programs that educate seafarers about the potential cyber security risks, the methods for identifying and mitigating these risks, and the importance of following best practices to ensure the safety and security of ship operations. The results emphasize the need for ongoing training and

[33] (Sørensen, 2023)

reinforcement of cyber security practices to keep seafarers informed and prepared to effectively respond to cyber threats. This is also underscored by DNV.

"*There needs to be more training made available for the staff. Training which is of a higher quality, and which is properly planned and being done on a regular basis will according to DNV heighten the quality of the personnels cyber security awareness".*[34]

According to DNV improper training will make personnel unaware actors in enhancing cyber-threats or "'friendly threat actors'" as DNV calls it. DNV recognizes a carelessness when we are untrained and unaware of the risks involved in cyber-attacks.[35]

The observations of DNV together with the results of the quantitative analysis proves a necessity for raising more cyber security awareness amongst the seafarers to mitigate the cyber risks. The literature also proves a need for more cyber security awareness training instead of focusing only on the internal mitigation strategies of the IT organization. Furthermore, the results underscore DNVs theory of the importance of collaboration between stakeholders in the maritime industry to address cyber security risks. Shipping companies should not be afraid of knowledge and experience sharing. This will enhance their cyber security robustness. These experiences can potentially be shared in secured maritime databases which is controlled and audited by the classification societies. The analysis emphasizes the need for cooperation between shipping companies, classification societies, regulatory bodies, and technology providers to develop and implement cyber security measures. The discussion highlights the significance of sharing information, best practices, and lessons learned to enhance the cyber security posture of the industry. This is also backed up by DNV which is a vital classification society organisation. Additionally, the results reveal the importance of continuous monitoring and proactive identification of cyber security risks. The analysis emphasizes the need for organizations to establish effective monitoring systems that detect and respond to potential cyber security incidents in a timely manner. It is therefore also vital

[34] (Veritas, 2023)
[35] (Veritas, 2023)

that the seafarers are getting the sufficient training to identify the cyber risks in a timely manner. The results emphasize the role of incident response and recovery plans in minimizing the impact of cyber security incidents and ensuring the prompt restoration of critical systems and operations. The seafarers must have easily accessible information of who to contact in case of an incident. It would also be recommendable to have a potential backup computer, which can access the various protocols, procedures, guidelines, and safety management systems in the event of a cyber security incident on board. The results also reflect the importance of having a robust incident response plan in place, which should include identification of key personnel and their roles during a cyber incident, steps to mitigate and contain the threat, and a communication plan to inform relevant parties about the incident. Furthermore, the plan should also include guidelines for the recovery of systems and data, ensuring these can be restored safely without the risk of further infiltrations. The quantitative data results also indicate a gap in knowing which actions to take in case of the IT systems onboard being compromised. 27,4% was either unaware or not sure what actions to take which underlines the importance of further identification and awareness training for the seafarers and a need for further information sharing in the organisations. Moreover, the findings point to the critical role of technology in enhancing cyber security in ship operations. The discussion emphasizes the need for organizations to stay abreast of the latest technological advancements in cyber security and adopt them as part of their mitigation strategies. This might include tools for intrusion detection, data encryption, and advanced threat intelligence, as well as technologies for automating certain security tasks, allowing for quicker detection and response to threats. The results also underline the challenges posed by the rapid evolution of cyber threats. Cybersecurity is a constantly moving target, with new types of attacks and vulnerabilities emerging all the time. This makes it crucial for maritime organizations to stay informed about the latest threats and to continuously update their security measures and strategies in response. They should also consider engaging external cyber security experts or services to ensure that they are getting the most up-to-date and expert advice.

14 CONCLUSION

14.1 Summary of the research and key findings

The research being conducted in this thesis focuses on the topic of cybersecurity in the maritime industry, particularly with regards to the awareness and training of seafarers. The aim of the research is to determine whether shipping companies are doing enough to improve cybersecurity awareness among seafarers, and to identify, mitigate, and assess the cybersecurity risks faced by seafarers and maritime organizations. Overall, the research being conducted in this thesis aims to contribute to the knowledge and understanding of cybersecurity in the maritime industry and to provide practical recommendations for enhancing cybersecurity practices and mitigating cyber risks among seafarers and maritime organizations.

14.2 Key findings

Many seafarers and employees in the maritime industry lack adequate awareness and training in cybersecurity best practices. This can lead to unintentional actions that expose the company and ships to cyber risks. Many companies lack comprehensive contingency plans and procedures to respond effectively to cyber incidents. This can result in delays in identifying and containing threats, leading to increased damages. There is a clear lack of consistent reporting and information sharing on cyber incidents in the maritime industry. This hampers collective efforts to learn from past incidents and improve cybersecurity practices. Based on these findings, it is recommended that maritime organizations increase investment in cybersecurity, enhance training and awareness programs, improve collaboration and information sharing. By addressing these key areas, the maritime industry can enhance its cybersecurity posture and mitigate the risks associated with cyber incidents.

14.3 Implications of the study

The implications of this study are significant for the maritime industry and its stakeholders. By examining the current state of cybersecurity awareness and measures among seafarers, the study aims to highlight the gaps and challenges in current cybersecurity practices. The study can help shipping companies understand the importance of improving cybersecurity awareness among seafarers. By identifying the current level of awareness and training, the study can provide insights into the areas that need improvement and the potential risks involved in ship operations. Through the identification of cyber threats and vulnerabilities, the study can assist in developing strategies for risk assessment and mitigation. By implementing these strategies, shipping companies can reduce the likelihood and impact of cyber incidents, safeguard critical systems, and ensure the safety of crew members and ship operations. The study can contribute to compliance with international guidelines and regulatory frameworks, such as those issued by the International Maritime Organization (IMO) and industry standards like ISO 27001. By aligning cybersecurity practices with these frameworks, shipping companies can demonstrate their commitment to cybersecurity and ensure compliance with industry standards. The study emphasizes the importance of collaboration and information sharing within the maritime industry. By promoting open discussion and sharing of experiences, best practices, and lessons learned, the study can facilitate the development of industry standards and guidelines, foster a culture of cybersecurity, and enhance the overall cybersecurity posture of the maritime industry. The study can serve as a foundation for future research and development in the field of maritime cybersecurity. By highlighting the gaps and challenges in current practices, the study can stimulate further research and innovation to address emerging threats, improve cybersecurity technologies, and enhance the resilience of the maritime industry against cyber incidents.

Overall, the implications of this study are focused on raising awareness, promoting effective risk management, and contributing to the academic and professional literature on cybersecurity in the maritime industry. The study aims

to provide valuable insights and recommendations to enhance cybersecurity practices and ensure the safety and security of maritime operations.

14.4 Concluding remarks

The topic focuses on the application of cybersecurity principles, practises, and frameworks in a ship operational context with specific emphasis on the maritime industry. It involves studying the threats, vulnerabilities and challenges that are associated with cyber risks in ship operations and it aims to develop strategies and solutions to safeguard critical systems, maintain operational reliability and ensure the safety of the ship and crew. In the face of an ever-evolving cyber threat landscape, this thesis project underscores the pressing need for a comprehensive, industry-specific approach to cybersecurity in the maritime industry. It is my hope that this work will contribute to efforts to create further awareness and safeguard the maritime industry against cyber threats, protecting the ships and their crew in commencing safe ship operations in the future. Based on the questionnaire results, it is evident that seafarers have a reasonable level of awareness about cyber security, however, there are areas where further education and training are needed, particularly in identifying and responding to potential cyber threats. Additionally, companies can play a more significant role in strengthening cyber security awareness among seafarers. In conclusion, the results of the analysis indicate that while there are significant challenges associated with cyber security in ship operations, there are also clear pathways for addressing these challenges. By raising awareness, fostering collaboration, implementing risk assessment and mitigation strategies, leveraging technology, and staying informed about the evolving threat landscape, maritime organizations can significantly enhance their resilience against cyber threats.

15 RECOMMMENDATIONS AND FUTURE WORK

15.1 Recommendations for enhancing cyber security awareness.

Based on the content of the thesis, here are some detailed recommendations for enhancing cyber security awareness in the maritime industry. Establish a training program that covers various aspects of cyber security, including recognizing phishing emails, creating strong passwords, identifying potential cyber threats, and reporting suspicious activities. Provide regular training sessions for all crew members and ensure that new employees receive training as part of their onboarding process. Foster a culture of cyber security awareness among all crew members. Encourage open communication about cyber security concerns, promote the reporting of potential vulnerabilities or incidents, and reward good cyber security practices. Conduct regular assessments of cyber security vulnerabilities and risks onboard ships. These assessments should include evaluating the effectiveness of existing security measures, identifying potential areas of improvement, and implementing necessary changes or updates to address any identified weaknesses. Implement strict access controls and user privileges to ensure that only authorized personnel have access to critical systems and data. Regularly review user access rights and revoke access for former employees or individuals who no longer require access. Regularly update and patch all shipboard systems, including software applications and operating systems, to protect against known vulnerabilities and exploits. Implement an effective patch management process to ensure that updates are applied in a timely manner. Encourage secure communication practices: Emphasize the importance of secure communication practices, such as using encrypted communication channels and avoiding sharing sensitive information over unsecured networks. Train crew members on secure communication protocols and provide them with the necessary tools and resources to ensure secure communication. Establish a comprehensive incident response plan that outlines the steps to be taken in the event of a cyber security incident. This plan should include procedures for identifying, containing, mitigating, and recovering from cyber security incidents. Regularly

test and update the incident response plan to ensure its effectiveness. Foster collaboration and information sharing: Encourage collaboration and information sharing among industry stakeholders, including ship operators, port authorities, and cyber security experts. Participate in industry forums and initiatives aimed at sharing best practices, lessons learned, and emerging trends in cyber security. It is important to continuously monitor the evolving cyber security threat landscape and stay updated on emerging threats and mitigation strategies. Establish channels for receiving timely cyber security alerts, advisories, and industry updates to ensure that crew members are aware of the latest trends and techniques used by cyber attackers. Conduct regular drills and exercises to test the effectiveness of cyber security measures and enhance the preparedness of the crew in responding to cyber security incidents. These drills can include simulated phishing attacks, incident response scenarios, and tabletop exercises to identify areas for improvement and increase cyber security awareness. By implementing these recommendations, the maritime industry can enhance cyber security awareness, improve the overall cyber security posture, and mitigate the risks associated with cyber threats.

15.2 Suggestions for future research.

Based on the recommendations provided, here are some potential areas for future research in enhancing cyber security awareness in the maritime industry. Research could be conducted to understand the effectiveness of various cyber security training methods and approaches in the maritime industry. This could include studying the impact of frequency, content, delivery methods, and assessing the retention and application of information among crew members. There is a need for more research on how to effectively foster a culture of cyber security among ship's crew. This could include qualitative studies on attitudes, behaviours, and barriers to creating a cyber-secure culture. Research could focus on developing and refining risk assessment methodologies tailored to maritime environments. This could help to create more accurate and comprehensive assessments of cyber threats. Investigating the most effective secure communication practices and tools in the maritime context could be beneficial.

This could include research into the usability and security of various encryption technologies and secure communication protocols. Research could be conducted to compare various cyber incident response strategies and their effectiveness in the maritime industry. This could also involve developing frameworks or models for effective incident response in maritime settings. It would be valuable to research how to best design and implement collaboration and information sharing mechanisms among maritime stakeholders. This could involve examining the challenges and benefits of various information-sharing models. Research should focus on understanding how best to keep pace with the continually evolving cyber threat landscape. This could include studies on predictive models for emerging threats, as well as exploring the application of AI and machine learning for threat detection and mitigation. Research could focus on understanding the effectiveness of various types of drills and exercises in preparing crew members for cyber incidents. This could involve studying how these drills and exercises could be better designed and executed for maximum impact. It would be beneficial to conduct longitudinal studies to evaluate the long-term effectiveness of implemented cyber security measures and their impact on the overall cyber resilience of maritime operations. Research into the psychological aspects of cyber security, such as user behaviour, attitudes towards security, and factors influencing security compliance, can provide valuable insights into improving cyber security awareness and practices in the maritime industry.

16 REFERENCES

- BIMCO and many others. (2020). *THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS.* BIMCO. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ANNEX%20Guidelines%20on%20Cyber%20Security%20Onboard%20Ships%20v.4.pdf

- Calder, A. (2005). ISO 27001/ISO 27002 A Pocket Guide. IT Governance Publishing. https://itgusa.blob.core.windows.net/files/download/2020-iso270002_1%20final%20ebook.pdf

- Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

- internatioal Association Of Classification Societies, (2022). Cyber resilience of on-board systems and equipment. IACS. https://www.american-club.com/files/files/ur-e27-new-apr-2022.pdf

- International Maritime Organisation. (2022). *GUIDELINES ON MARITIME CYBER RISK MANAGEMENT.* IMO. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

- International Maritime Organisation. (2017). MSC.428(98). MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS. IMO. *https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.* https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

- International Assosociation of Classification Societies,(2022). IACS. Cyber Resilience of Ships. https://www.american-club.com/files/files/ur-e26-new-apr-2022.pdf

- International Association of Classification Societies,(2020). Recommendation on cyber resilience. IACS. https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/24150438/rec-166-corr2-apr-2022-ul.pdf

- Sørensen, René. (2023). Appendix Questionnaire. https://docs.google.com/forms/d/e/1FAIpQLSf2S1VHHuvla5PG75oikyAaDDM-b9DQmuA8NU2yYO5J2LMuOA/viewform.

- DNV Det Norske Veritas, (2023). Maritime Cyber Priority 2023. DNV. https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.html

17 APPENDIX

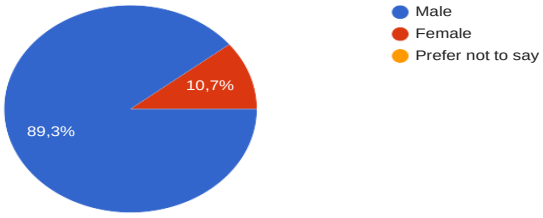
Enhancing Cyber Security Awareness Among Seafarers

84 svar

Gender

Kopiér

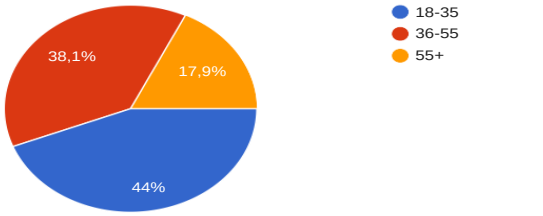
84 svar



Age

Kopiér

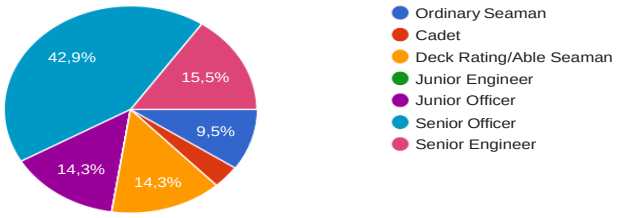
84 svar



Rank

Kopiér

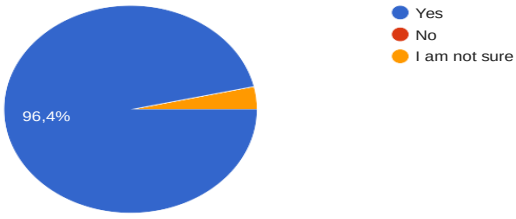
84 svar



Do you understand what cyber security is and why it's important?

Kopiér

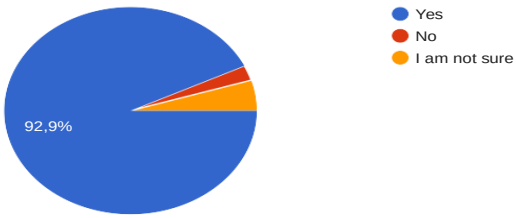
84 svar



Are you aware of the cyber security policies and procedures in your company?

Kopiér

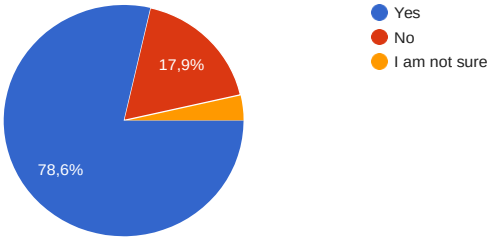
84 svar



Have you ever received any training or education on cyber security?

Kopiér

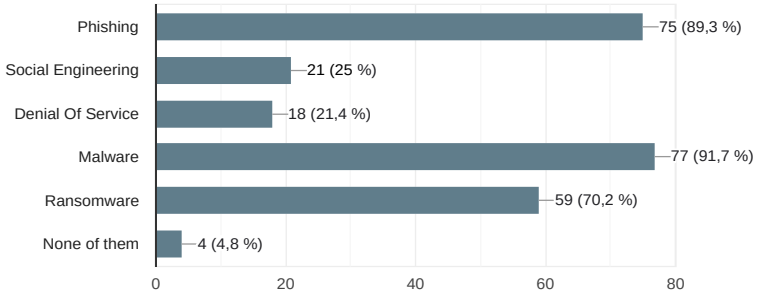
84 svar



How many of these cyber threats do you recognize? (Tick of the ones you know)

Kopiér

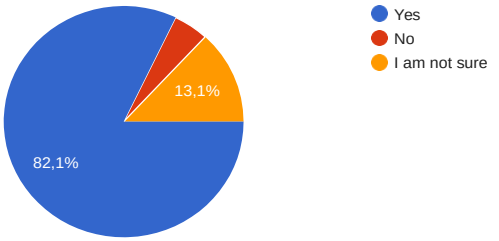
84 svar



Do you know how to identify a phishing e-mail or a malicious website?

Kopiér

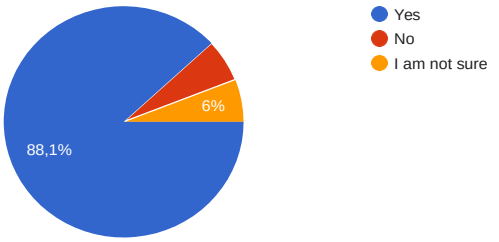
84 svar



In case of a suspected cyber security incident, do you know who to contact and which actions to take?

Kopiér

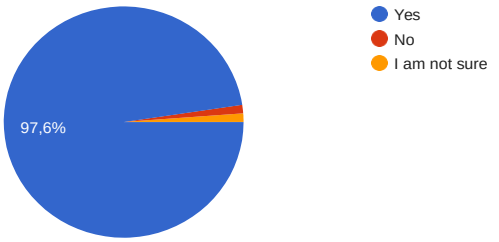
84 svar



Are you aware that portable devices (such as USB-drives, smartphones, etc.) can be the source of cyber threats?

Kopiér

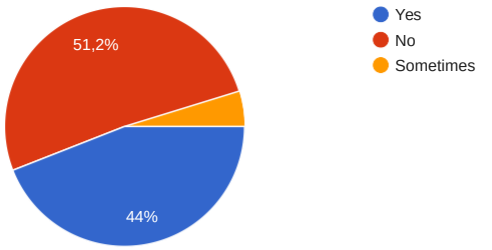
84 svar



Do you connect your personal devices (such as your personal phone) to the ship's network?

Kopiér

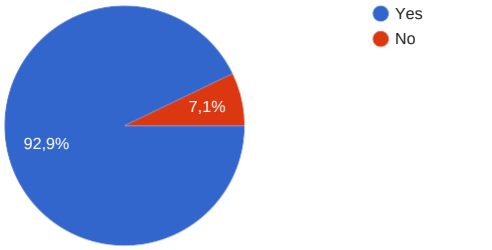
84 svar



Are you aware that sharing sensitive information while connected to an unsecure network can lead to security breaches?

Kopiér

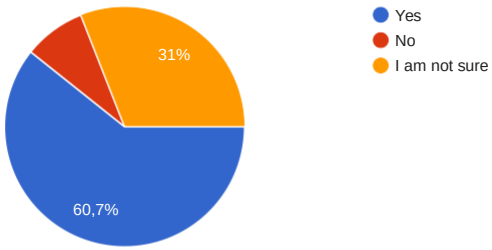
84 svar



Do you know how to identify unusual activity or potential signs of security breaches?

Kopiér

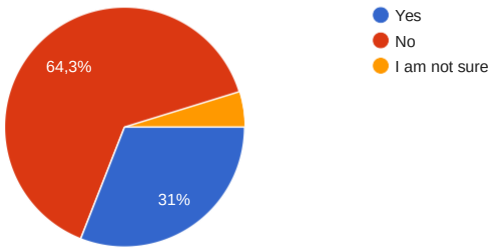
84 svar



Have you ever noticed any unusual activity or potential signs of cyber security breaches on the ship's network?

Kopiér

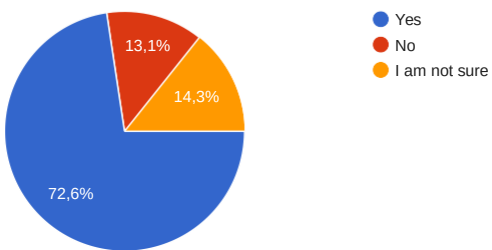
84 svar

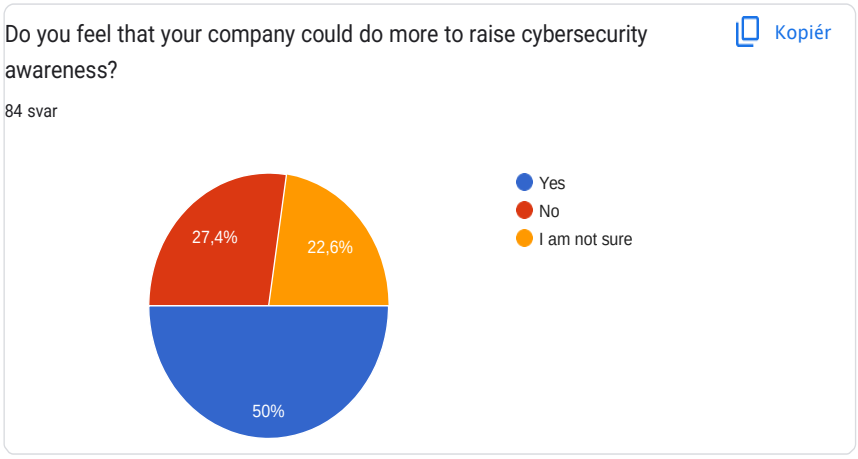


Do you know which actions to take if your ship's IT, navigation, communication or operation systems show signs of being compromised?

Kopiér

84 svar





36

[36] (Sørensen, 2023)