An investigation into cyber security risk mitigation and the human factor in developing a cyber security culture

A comparative analysis of two maritime companies in Norway

Candidate name: Synne Skoe Strand

University of South-Eastern Norway
Faculty of Technology, Natural Sciences and Maritime Sciences

MASTER THESIS

May 2023

Abstract

Throughout the years the number of cyber-attacks towards the maritime industry has increased rapidly. As the maritime industry is the most important industry when it comes to the transportation of cargo and energy a cyber-attack has the potential to inflict severe disruption upon the supply chain. The objective of this study is to conduct an analysis of two maritime companies located in Norway, investigating the participants knowledge and behaviours contributing as human factors shaping the companies cyber security culture. The aim for this research is to assess the risk mitigation measures implemented by the two selected companies in response to cyber threats. 5 employees from two separate companies were interviewed and there was performed an analysis on the results of 10 individual interviews. The results of the research show that there is a lot of information and guidelines regarding cyber security on the intranet of each company, however not all the employees check this site and therefore is not aware of the information and guidelines. In addition, communication from senior management regarding this issue is low and most of the information comes through the IT department. Also, it was detected that onboarding cyber security training was at high priority, however the yearly training and awareness courses varied. Therefore, the study proposes as solutions for a "cyber security champion" in every office in the organization to help improve the awareness and make sure that all of the employees understand the guidelines. In addition, the study suggests expanding this research to several companies within the maritime industry and also implement the employees that works onboard the ships to get an overview of the whole industry.

Acknowledgments

I want to thank associate professor. Marius Imset, my supervisor, for his advice, expertise, and assistance during this master thesis process. I sincerely appreciate all of your help and guidance. I also want to express my gratitude to University of South-Eastern Norway for the two years, a ton of new knowledge, and a lot of new friends. Additionally, I want to thank the companies that supported my thesis by taking out time from their hectic schedules to participate in interviews. Last but not least, I want to thank my friends and family for their motivation and support during this master's program.

Acronyms

APT Advanced persistent threat

DoS Denial of service

ENISA European Network and Information Security Agency

GDPR General data Protection Regulation

ICS International Chamber of Shipping

IMO International Maritime Organization

ISM The International Management Code for the Safe Operation of Ships and for Pollution Prevention

ISMS Information security management

IT Information Technology

NSD Norwegian Center for Research Data

OT Operational Technology

RQ Research question

UNCTAD United Nations Conference on Trade and Development

VPN Virtual Private Network

Table of contents

1. Chapter I - Introduction

For hundreds of years the world trade and economy have been depended on the maritime industry to transports cargo, energy and passengers around the world. According to International Chamber of Shipping (ICS) up to 90% of the world trade is carried out by the international maritime sector. On a yearly basis the maritime sector handle 11 billion tons of cargo with more than 50.000 ships and employs 1.5 million sailors (International Chamber of Shipping , 2023). Norway is one of the largest offshore shipping nations in the world, and for more than 150 years, Norway has been a significant player in both the shipping and shipbuilding industries. (International Trade Administration, 2022).

Health, safety and environmental risk in the maritime industry is no longer only related to physical unwanted incidents such as motor accidents, grounding or pirates. Due to digitalization and modern technology ships are well equipped with computer systems that can be hacked. This increases the possibility for cyber-attacks, which can disrupt operations, steal sensitive information, and even cause physical damage to ships, ports, cargo and in worst case loss of life. One of the biggest and fastest growing threats to today's international maritime organizations is the cyber risks and attacks. The average age of the worldwide fleet, measured in terms of the number of ships, was 21.29 years according to data provided at the United Nations Conference on Trade and Development (UNCTAD) at the beginning of 2020, and 41,85% of all ships currently at sea are older than 20 years. This indicates that the majority of these ships are much likely currently sailing with outmoded and vulnerable operational technology (OT) infrastructure because there was no cybersecurity by design provision at the time of their construction (United Nations Conference on Trade and Development, 2020). Ships that sail with old and outdated operating systems are more vulnerable to cyber-attacks. (Martin & Hopcraft, 2020) According to Allianz's Safety and Shipping Review from 2020, the number of attempted cyber-attacks against marine sector companies has increased by 400% since the Covid epidemic started (Kechagias, Chatzistelios, Papadopoulos, & Apostolou, 2022).

There is no measure or prevention tool that can give a 100% protection from cyber-attacks. However, there are a lot of measures that can be implemented to mitigate the risk considerably. According to the International Maritime Organization (IMO) one of the key challenges in improving cyber security in the maritime industry is the lack of awareness and training among industry professionals. Many maritime organizations do not have the necessary expertise or resources to effectively manage and respond to cyber threats, and many workers lack the training and knowledge they need to understand the risks and how to protect themselves and their organizations from attacks (International Maritime Organization, 2017). The maritime industry needs to prioritize cyber security and invest time and money in relevant expertise to implement this effectively throughout the whole organization. The standards and framework are widely available, however, this is not prioritized (Cyber Risk GmbH , 2020). A report from European Network and Information Security Agency (ENISA) names low awareness as the first vulnerable point of the industry regarding cyber security (Cimpean, et al., 2011).

To address the challenges related to cyber security, IMO has recommended that maritime organizations invest in training for all of their employees. This training should include an overview of the current state of cyber security in the maritime industry, and an understanding of the types of cyber threats that organizations face, in addition to best practices for avoiding and mitigating these threats. Furthermore, IMO has called for the development of industry-wide training programs to provide maritime workers with the skills and knowledge they need to effectively manage and respond to cyber threats. In April 2017, IMO issued guidelines on maritime cyber risk management. These guidelines highlighted the importance of senior management involvement when it comes to creating a culture of cyber risk awareness into all levels of an organization (International Maritime Organization, 2017).

In the recent years cyber security in the maritime industry has also been a prioritization in Norway by the Norwegian companies, agents and authorities. In 2020 a draft of a maritime cyber security strategy was developed by the Norwegian Maritime Authority in cooperation with the Norwegian Coastal Administration and representatives from the Norwegian National Security Authority. The draft addresses goals, risks and potential threats and outlines measures to achieve a cyber security safety in the maritime industry. The overall goals of this strategy are broken down into five separate goals. The first one is to ensure the reliability and safety of the digitization that is taking place in the maritime industry. The second goal is to provide a trustworthy and protected digital infrastructure to the maritime sector so that it can thrive. The third goal is to improve the marine industry's capacity to recognize, respond to, and prevent cyber-attacks through increased cooperation and the sharing of expertise. The fourth goal is to provide individual participants in the maritime industry with the tools necessary to defend themselves against cyber-attacks. The last one is to ensure that crew members and workers have the capabilities in terms of cyber security. (Norwegian Maritime Authority, 2022)

The human factor and awareness in every level of the organization plays a crucial role in mitigating the risk of cyber-attacks. It is therefore important to focus on promoting a culture of cyber security awareness and best practices throughout an organization that’s start at the top with senior management. Classification society such as DNV pointed out the importance of securing process, people and new technology. They state that it is critical to train the employees, perform emergency drills and define roles and responsibility. (DNV, 2023)

1.1 Purpose of the research

This thesis investigates the human factor when it comes to mitigating cyber-attacks and how an organization should focus on building a proactive cyber security culture. The focus will be on the onshore employees with various positions within the two maritime companies. Furthermore, this thesis aims to examining the current state of knowledge and practice in this field, identifying gaps and challenges, and proposing solutions to improve the industry's resilience to cyber threats.

1.2 Research questions

The research questions (RQ) of this research study are:

RQ1: What mitigating actions have been implemented by the two Norwegian shipping companies to prevent successful cyber-attacks?

RQ2: What does onshore employees in the two maritime companies in Norway do to improve their cyber security awareness?

RQ3: How does the two maritime companies create a culture that emphasis cyber security awareness and training?

RQ:4 How does senior management work to play a more active role in creating and carrying out cyber safety measures?

1.3Thesis structure

Including the introduction, the thesis is structured into six chapters. After the introduction, chapter two will present a literature review that provides a deeper understanding to the relevance of cyber security. Chapter three will present methodology this includes the data, sample, measures and analysis. Furthermore, chapter four will present findings and then this will be discussed in chapter five. Last, chapter six will give the concluding remark and limitations of the thesis, followed by suggestions for measures that maritime companies should implement in order till strengthen their cyber security.

2. Chapter II – Literature review

2.1 Purpose of the literature review

The aim of the literature review is to develop a greater understanding of cyber security, current issues, various attack types, and strategies for reducing the risk of a cyber-attack in a maritime organization. Furthermore, how the human factor in an organizational culture and cyber security awareness within an organization plays an important role when it comes to mitigating a cyber-attack. In addition, this literature review is to give insight to earlier studies that have been conducted in the field as well as the theories and techniques that have been applied in this research. This provides an outline of the current base of information and enables a critical assessment to identify any research gaps in the area.

2.2 Method used for the literature review

Search engines such as Oria and Scopus were applied when attempting to locate relevant and trustworthy sources. This included relevant books, reports, and articles. In addition, past lectures provided additional materials. Finding literature that emphasized the value of human factors and organization culture in relation to cyber security was the main objective. The following list contains search keywords that were used:

- Cyber security
- Human factor in cyber security
- Organization culture
- Developing a cyber security culture

This was beneficial because it focused on the information that was most relevant to this topic. The strongest sources that were relevant and trustworthy was identified next. As a result, articles and reports from reputable publications and businesses were used. The literature was identified, assessed, and then thoroughly read before being used.

2.3 Different types of cyber-attacks

The following section will provide insight into different types of cyber-attacks that may affect companies and ships:

Untargeted attacks

These types of attacks access internet-based tools and methods that can be used to find, identify, and exploit vulnerabilities that exist in a business or on board a ship. (BIMCO, 2021)

Malware

Malware is known as software that can access or harm a computer without the owner's knowledge. Malware comes in a variety of forms, including viruses, worms, trojans, spyware, and ransomware. Data on systems is encrypted by ransomware until a ransom is paid. Additionally, malware may take advantage of flaws and issues with out-of-date or commercial software. Typically, the use of software or code intended to control and profit from a flaw in another computer hardware or software is referred to as "exploiting." (BIMCO, 2021).

Water holing

Creating a fake website or compromising an actual website to take advantage of users (BIMCO, 2021).

Scanning

Searching the internet at random for exploitable weaknesses (BIMCO, 2021).

Typo squatting

Known as URL hijacking or fake URL. This type of unwanted cyber-attack relies on errors made by internet users when entering a website address through a web browser, such as typos. If a user mistakenly types in the wrong website address, they could be redirected to another fraudulent website (BIMCO, 2021).

Targeted attacks

This type of attack may be more advanced and employ tools and strategies made especially for targeting a specific organization or ship.

Phishing

Requesting specific sensitive or confidential information by email to a huge number of possible targets. A malware file or a request to visit a phony website via a URL could also be included in the email (BIMCO, 2021).

Social engineering

A non-technical method that potential cyber attackers employ to trick insiders into circumventing security measures, typically but not always through social media contact (BIMCO, 2021).

Brute force

This type of approach attempts countless passwords in the intention of successfully guessing the right one. In order to find the right password, the attacker thoroughly checks each one (BIMCO, 2021).

Credential stuffing

Attempting to gain unlawful access to a network or business using credentials that have already been hacked or certain widely used passwords (BIMCO, 2021).

Spear-phishing

Similar to phishing, however the targets are sent personal emails that frequently contain dangerous software or links that instantly download malicious software. Signals have occasionally been utilized to create a feeling of familiarity with an email address (BIMCO, 2021).

Denial of service (DoS)

Blocks access to information by authentic and permitted users, typically by saturating a network with data. A distributed denial of service (DDoS) strike uses several servers or machines under its control to commit a denial of service attack (BIMCO, 2021).

Subverting the supply chain

Attacking a business or ship by compromising the hardware, software, or support services being sent there (BIMCO, 2021).

2.4 Threat Actors

Maritime companies need to be aware of the various threat actors, as well as their capacity, opportunity, and attack-related motivations. They must also think about the impact of a potential attack, the possibility that it will happen, and the risk element involved, in addition to how a potential attacker would have a reason to strike the organization. Organizations and individuals may pose a threat to the company, crew's safety and security, the environment, and the ship (BIMCO, 2021). These threat actors may choose to hack a company for a variety of reasons. Financial gain is the primary and most frequent motivation. They can accomplish this in a number of methods, but the most popular ones involve gaining access to a bank or investment account, tricking an employee into transferring money by using a phishing scheme, or launching a ransomware attack on the entire business (Mottl, 2022). The following definitions of threat actors will explain who they are and their motivation.

State-sponsored cyber threat actors

These threat actors operate on behalf of nation-states to disrupt critical infrastructure or building networks, hack devices, and facilitate additional cyber threat activity to advance political goals. They could also engage in threat behavior with financial motivation. They usually have extensive staff and resources, and they carefully plot and coordinate their attacks (Boyes & Isbell, 2017). By attacking the maritime industry, the state-sponsored cyber threat actors can disrupt different supply chains that can be critical for a country or a company.

Terrorists

The use of IT by terrorists is growing, and they already use the internet extensively for communications and propaganda distribution. Since electronic and computer-based technologies are so widely used in maritime environments, terrorist organizations may be able to exploit the many toolkits that are available for download to disrupt or destroy ships by attacking ship or connected shore-based systems. Their motivation might be financial gain, create fear or disrupt critical infrastructure (Boyes & Isbell, 2017).

Cyber Criminals

Cyber criminals are highly skilled criminal organizations that engage in a variety of IT-enabled crimes. The goal is to make money through illegal behavior, and they have primarily focused on fraud, account thefts, and thefts of intellectual property. However, in addition to using malware to encrypt data or threatening denial of service attacks on corporate websites, cybercriminals often engage in blackmail. Cybercriminals may attempt to intercept or get access to information on cargo shipments or security measures in relation to ports as a lead up to criminal activities or a physical attack on these premises (Boyes & Isbell, 2017**).**

Competitors

Competitors often consists of firms looking to get an edge over another company competing in the same industry and get access to inside information. The goal of their actions is to harm a competitor by obtaining business intelligence, stealing intellectual property, gathering competitive intelligence on bids, or interrupting operations to cause financial or reputational loss. They may act alone or through third parties. Depending on their size, industry, location, and level of cyber competence, huge corporations may be able to carry out sophisticated operations to target and compromise their rivals (Boyes & Isbell, 2017).

Activist groups

These groups, which are frequently referred to as hacktivists, are made up of ideologically driven individuals who could create flexible groups or subgroups. Their actions basically amount to online demonstrations with the intention of disrupting systems or obtaining private or sensitive material for publication or dissemination in order to put their target in the public eye (Boyes & Isbell, 2017).

An individual

The sophistication and motivation of an individual can vary greatly. Some of them might be decent people who don't want to hurt the business but gets trick or pressured into doing it. However, it may be a disgruntled worker with little IT expertise or a disgruntled worker with a lot of IT expertise. Cyber criminals may also be involved if they're only wanting to demonstrate their IT skills and not for financial gain. Another possibility is a lone wolf, who is an individual with advanced technical knowledge who operates independently of the organization. This group might be skilled at erasing records of their actions, for as by deleting or changing entries in system logs (Boyes & Isbell, 2017).

2.5 Maritime cyber-attack incidents

Industry-specific cyber-attacks are a reality and over the years there have been several attacks to ports, ships and other data breaches. Cyberthreats and weaknesses might allow hackers to access logistical software, exploit bank records, and take over ship navigation and engine controls. In this section, we look into different cyber-attacks that has accord in the recent years in the maritime industry:

Icefog

According to a report published by Kaspersky, an advanced persistent threat (APT) known as an interactive espionage tool has been in operation since at least 2011. The tool, which is directly controlled by malicious actors, has primarily targeted shipping companies and governmental institutions located in Japan and South Korea. APTs are a significant concern for organizations and governments due to their persistence and ability to evade detection. The spear phishing emails used in the icefog targeted cyber-attacks aim to lure the victim into accessing a malicious attachment or webpage. Microsoft Office documents (Word and Excel) that drop and execute the backdoor and display a phony document to the victim are used to exploit the first two vulnerabilities. These tend to be the attack strategies that are now most frequently used by the attackers (Kaspersky Lab, 2013).

NotPetya

Employees at A.P. Moller-Maersk began receiving notifications in June 2017 that their file systems were being fixed, while others received notifications that their crucial files were being encrypted. This marked the beginning of NotPetya's hacks into Maersk and a number of other multinational corporations (Capano, 2021). NotPetya successfully infiltrated a single computer in Odessa, which provided the attackers with the necessary access to compromise the entire system. As a result, critical components such as port facilities, booking systems, and container loading systems, which are crucial to prevent ship capsizing, were brought to a halt. In response, Maersk formed an incident response team and established a recovery center to minimize the impact and facilitate the recovery process. This recovery operation involved hundreds of workers operating around the clock globally. Eventually, Maersk personnel discovered a backup in their Ghana office. Luckily, a power blackout had caused the server to disconnect from the network prior to the NotPetya attack, preserving a single clean copy of the company's domain controller data. The recovery team found the discovery of this backup to be a source of relief. Ultimately, the estimated cost of the attack to Maersk ranged between $250 million and $300 million (Capano, 2021).

Port of Antwerp

A cyberattack was launched against two businesses that were based in the Antwerp port between June 2011 and June 2013 by an organized crime group operating in Belgium. The organization was able to gain access to sensitive security information about the containers in the port after successfully breaching the computer networks of the targeted businesses. Such access enabled the group to steal cargo before the legitimate owners could take possession. Additionally, the criminals exploited the security loophole to smuggle drugs into the country via the port. The breach was identified by the port authorities when entire containers were missing. During a police raid on the group, authorities discovered more than a ton of cocaine with a street value of 130 million pounds, and a similar quantity of heroin (Bateman, 2013).

GPS Spoofing

GPS spoofing is a form of cyber-attack that involves the transmission of false GPS signals to a targeted system, resulting in the provision of incorrect navigational data. In the c the maritime industry, this can have dangerous conserveness such as navigational errors, vessel collisions, and groundings (Lo, 2019). GPS spoofing has become an increasingly prevalent threat to the maritime industry, as evidenced by a recent incident in the Black Sea. Several ships in the area reported unusual GPS readings at various times in late June 2017, with their location being incorrectly identified as being at an airport. These occurrences have highlighted the possible dangers posed by GPS spoofing and prompted worries about cyber-attacks (Jones, 2017).

2.6 What is cyber security and cyber risk management?

Computers, phones, tablets, and navigational systems are some of the few smart devices that are generally connected to the internet nowadays. Our availability to always be reachable, communicate with people anywhere in the world, and pinpoint and track our whereabouts are some of the advantages of this. However, connectivity carries a certain amount of risk. The internet can connect to us when we can connect to it.

“Cyber security is how individuals and organizations reduce the risk of cyber-attack” (National Cyber Security Centre, 2023). Everyone needs to be aware of the threat posed by cyber-attacks, including those working in the maritime sector. In the maritime industry we can categorize cyber systems into two groups: standard information systems (IT), which are more focused on information security and employ information security management (ISMS) onshore. However, Operation and Control system (OT) is less developed when it comes to cyber security, and a cyberattack on onboard OT system may threaten the safety of the ship and the crew (DNV, 2023).

When examining the characteristics of the maritime industry that make it particularly exposed to cyber security threats and desirable to hackers, the following might be mentioned. Due to the part of a lack of awareness and understanding among operators and managers, the maritime industry is having difficulties managing cyber risk. The industry is especially vulnerable to cyber-attacks because of the risks posed by connected technologies. Another factor contributing to the challenges of cyber risk management in the maritime industry is the complex network of parties involved in the operation of a ship. This can lead to a lack of accountability for ensuring the security of the ship's systems and data. (Kechagias, Chatzistelios, Papadopoulos, & Apostolou, 2022) Onboard ships, there is a larger danger of cyber-attacks due to increased usage of digital tools for communication and automation. In order to prevent unintended consequences, cooperation and experience exchange are essential. Cybersecurity has become a required component of safety management for ships and shipping companies from the first of January 2021. Cybersecurity is now a component of ISM audits (Norwegian Maritime Authority, 2022).

In addition to the lack of awareness and accountability, the maritime industry also involves a large number of interconnected businesses and authorities that communicate sensitive information, such as business critical, data sensitive, and commercially sensitive information. Because of the numerous potential entrance points this gives cybercriminals, it is even more crucial to take measures to protect the industry from attacks. Large financial transactions that occur often in the maritime industry's day-to-day operations further highlight the necessity for efficient cyber risk management procedures. The ability to safeguard these transactions, and the sensitive information they involve, is critical to the continued success of the industry. (Kechagias, Chatzistelios, Papadopoulos, & Apostolou, 2022)

A company must work hard to develop, implement, and maintain a cyber risk management program. Senior management must therefore be involved throughout the entire process to make sure that protection and contingency planning are calibrated to manage risks within a reasonable range. Cyber threats have the potential to harm the company's performance and reputation as well as the environment's and employees' safety. Therefore, a cyber risk is as much of a business challenge as a safety challenge. (BIMCO, 2021) Cybersecurity improvements could be time- and expensive for businesses. It might also affect how the company deals with its various stakeholders, including clients, suppliers, and authorities. (BIMCO, 2021)

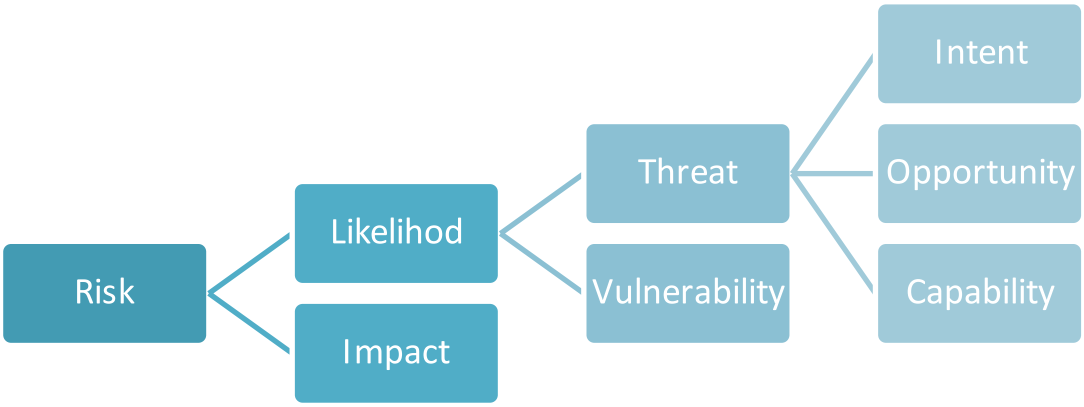

Figure 1: The relationship between different factors influencing the risk.

It is important that senior management take on an active role in overseeing cyber security measures within their organization, rather than responding only when significant findings or incidents arise. In order to achieve this objective, senior management must collaborate with mid-management to establish a cross-functional cyber security group, which includes relevant stakeholders. This will require the creation of a supportive workforce that is well-informed and equipped with the necessary awareness programs and training to apply them effectively. Additionally, by adopting efficient security governance, user awareness and training programs, and a framework for ongoing review and development of their security culture, companies can foster a security culture that is supportive of positive models and outcomes. Senior management should prioritize the creation of open lines of communication and cooperation in order to ensure that all employees are appropriately informed about and participate in the organization's cyber security initiatives. They should also foster an atmosphere of accountability and responsibility where all employees are encouraged to actively participate to the upkeep of the organization's security and feel empowered to report any known vulnerabilities or flaws. (Blum, 2020)

In April 2017 IMO issued guidelines on maritime cyber risk management. These guidelines outline the essential components needed to handle cyber risk in an efficient manner.

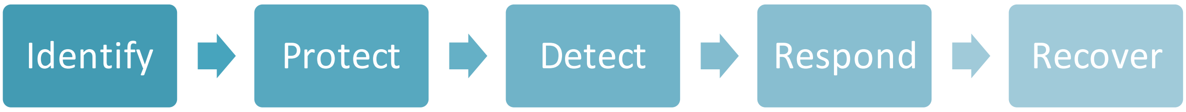

Figure 2: Cyber risk essential components

The implementation of a cyber risk management framework for the shipping industry must begin with the identification of personnel responsible for overseeing the process. The relevant personnel should conduct a thorough assessment of the systems, assets, data, and capabilities that, if disrupted, would pose a threat to the operation of the ship.

The second stage of the framework is protection. In order to safeguard the security of the systems, steps must be made to build risk control procedures and create a backup plan in case of a cyber-attack. This plan has to contain steps for making sure shipping operations continue even in the event of a cyber-attack.

The third stage is detection. It is critical to create and implement the required procedures to identify in order to ensure prompt response to a potential cyber-attack. By installing monitoring and surveillance devices to look for suspicious activities, this can be accomplished.

The fourth stage is response. It is crucial to have a solid plan in place to offer resilience and restore the vital systems required for the continuation of maritime operations in the event of a cyber-attack. This should include steps taken to lessen the effects of the attack, prioritize recovery operations, and guarantee the swiftest possible restoration of vital systems.

The final stage is recovery. After a cyberattack, it's critical to figure out what steps to take to backup and restore the systems so they can keep working. This should include the adoption of business continuity plans, disaster recovery planning, and the deployment of efficient backup and restoration systems. (International Maritime Organization, 2017)

2.7 The human factor within an organization

The human factor in the context of cyber security describes the role people play in preventing, detecting and responding to cyber security incidents (Schultz, 2005). The human factor is often cited as a major vulnerability in cyber security, where cybercriminals employ social engineering tactics to exploit human weaknesses and vulnerabilities (Corradini & Nardelli, 2019). Hence, it is crucial to ensure that senior management prioritize cyber security and awareness training within the organization. This secures that personnel at all levels of an organization has a sufficient understanding of cyber security and are trained to identify and respond appropriately to potential threats (BIMCO, 2021). The head of Maritime Technology Regulation at BIMCO stated: "80% of the cybersecurity incidents could have been prevented if a single user were able to recognize the threat. It is vitally important to educate the crew on board in order to rase awareness about vulnerabilities arising from human error" (Lagouvardou, 2018). There could be other reasons of human mistake, such as "Unfamiliarity," which is a condition that is significant but occurs infrequently, or "Understanding," which means a lack of availability to deliver information in a way that is easy to understand (Khripunov, 2023).

Tischer conducted a social experiment which revealed that when memory sticks were deliberately dropped in a random manner on a campus, an overwhelming 98% of them were subsequently connected to a computer. However, Bullèe conducted a separate experiment which demonstrated that interventions in the form of cyber security culture initiatives, such as posters, emails, or warning labels, were effective in reducing the success rate of such attacks (Hopcraft, Tam, Misas, Moara-Nkwe, & Jones, 2022).

Hugh Boyes and Roy Isbell have also highlighted that humans are often the most vulnerable point in any secure system or operation involving people within the ship system. Therefore, it is essential to comprehend the decision-making process of selecting appropriate mitigation measures. This involves identifying the individuals who require access to the ship data and systems, and the specific type of access needed. Furthermore, it is important to consider the level of cyber security awareness and understanding required by these individuals. It is also imperative to assess whether contractors, temporary staff, and agency workers are provided with adequate cyber security awareness training as part of their induction. (Boyes & Isbell, 2017)

Stated in a report by the ISACA/CMMI Institute, there exists a discrepancy between the present and desired state of an organization's cyber security culture. They conducted a survey with 4 800 business and technology professionals that replied via online polling. Respondents revealed that a significant gap was identified by 32% of participants, while 63% of respondents reported a minor gap, and the remaining 5% reported no gap between the present and desired state of cyber security culture. These findings suggest that a significant proportion of organizations may not have fully developed cyber security cultures, which could potentially leave them vulnerable to cyber-attacks (The ISACA/CMMI Institute, 2022).

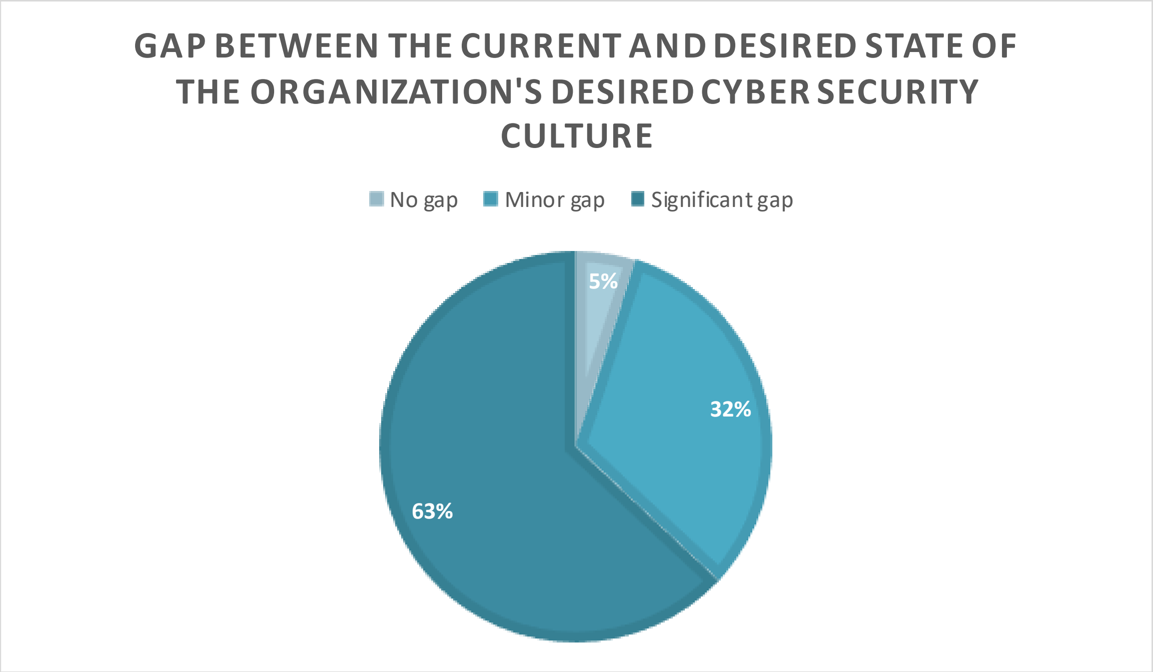

Figure 3: Gap between the current and desired state of the organization's desired cyber security culture

2.8 Role of management

It is critical that senior management recognizes the value of the human factor within the company as a whole. When developing a cyber security culture, they must keep this in mind. According to Matt Mayberry, leaders must explain the vision at the outset of developing a new culture. They must also show the way forward in order to overcome resistance and actually shift the course of events. They additionally have to incorporate and prioritize continuing and regular coaching and training (Mayberry, 2023). As mention before “80% of the cybersecurity incidents could have been prevented if a single user were able to recognize the threat” (Lagouvardou, 2018). Based on this information, it is critical to emphasize the importance of well-trained staff. Training is typically designed to teach a new skill or improve performance on a certain job. Training should be a systemic approach in order to keep or improve the performance standards within the existing competence framework (Khripunov, 2023). When implementing training programs, top management should prioritize the development of practical and operational knowledge and skills among all employees. Improve communication through clarifying organizational structures, roles, duties, and authority. It is also critical to focus on both knowledge-based and skill-based training, as well as to assure the quality and effectiveness of the training for the employees being trained (Khripunov, 2023).

2.9 Reframing organization culture

The following section provides insights into various tasks and approaches that could be beneficial for senior management to adopt, with the objective of enhancing their skills as managers and reframing organizational culture. Organizational change is a complex and challenging process that is often met with resistance. According to a survey conducted by Bain and Company on 250 American companies, only 12% of them successfully achieved their intended changes. The majority of companies, 38%, failed to achieve even half of their goals, while the remaining 50% settled for a significant shortfall. (Bolman & Deal, 2017)

Resistance to change is common and often reasonable, as new methods may represent a management that takes the organization in the wrong direction. Furthermore, changes in routine practice and protocol can undermine existing knowledge and skills, which can undermine people's confidence and ability to perform successfully. (Bolman & Deal, 2017)

When implementing a cyber security culture within an organization, it is crucial to address resistance to change. By offering training, psychological support, and opportunities for participation to increase people's understanding and comfort with new methods resistance can be eliminated. In addition, it is important to listen to the employee's ideas and concerns. Furthermore, to make sure that the employees have the necessary talent, confidence, and expertise to carry out their new responsibilities (Bolman & Deal, 2017).

2.10 Change Strategy within an organization

According to John Knotter, the process of innovating a company strategy is divided into eight steps that require a considerable amount of time to complete. Skipping any of these steps may lead to the illusion of speed, but rarely produces sufficient results. The first step involves creating a sense of urgency by identifying and discussing crises, potential crises, or major opportunities. The second step involves putting together a guiding team that possesses the necessary skills, credibility, connections, and authority to drive the change process forward. The third step entails developing a vision and strategies for achieving it. The fourth step involves communicating the vision and strategy through a combination of words, and actions. The fifth step involves either removing obstacles or empowering individuals to progress. The sixth step involves planning for and creating short-term wins, recognizing and rewarding employees involved in the improvements (Kotter, 1995).

The second to last step requires staying committed to the process and refusing to quit when difficulties arise. Finally, the last step is to foster and shape a new culture that supports innovative ways (Kotter, 1995).

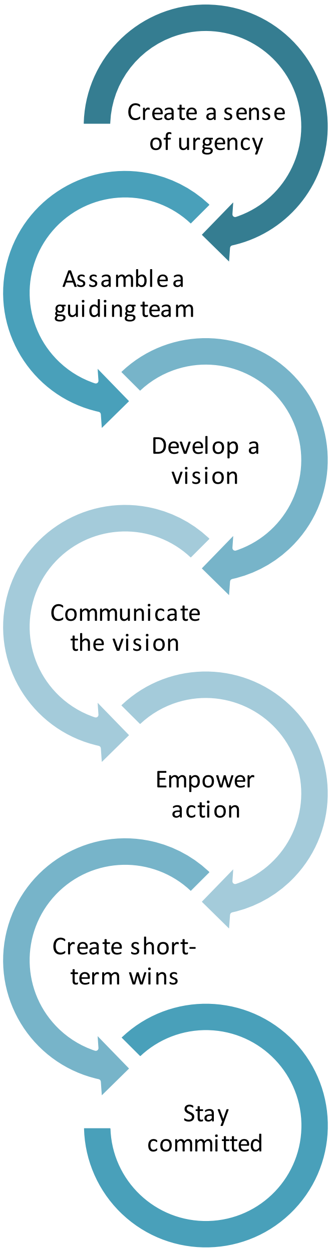

Figure 4: Change strategy by John Knotter

These steps can be linked to the International Maritime Organization (IMO) guidelines regarding cyber security. In particular, the first step of creating a sense of urgency can be linked to the IMO guidelines' emphasis on risk assessment and management. Similarly, the second step of assembling a guiding team with the necessary skills, credibility, connections, and authority aligns with the IMO guidelines' call for designated personnel to manage cyber risk. The third step of developing a vision and strategies can be linked to the IMO guidelines' emphasis on establishing appropriate cyber security policies and procedures. The remaining steps align with the IMO guidelines' recommendations to raise cyber security awareness, develop and implement training programs, and establish procedures for monitoring and reviewing cyber security practices (International Maritime Organization, 2017). Cyber security breaches can arise as a result of human error or misconduct. This is often connected to insufficient training and awareness. Therefore, it is important that senior management establish a defined vision and objective for the implementation of a cyber security safety culture within the organization. The focus on developing a cyber security safety culture, serves to mitigate the risks posed by the human element to cyber security and to enable employees to function as resilient human firewalls (Hopcraft, Tam, Misas, Moara-Nkwe, & Jones, 2022).

In a company, it is common to encounter resistance to change. It is therefore important for management to anticipate and understand the extent and nature of resistance. Strategies for managing resistance to change may vary, depending on the underlying reasons for the resistance. If resistance is rooted in a lack of information, education can be used to communicate the importance for the desired change. Through education, individuals may become more receptive to the proposed changes. In situations where resisters require greater motivation, involving them in the design or implementation of the change may increase their commitment. Additionally, if individuals feel unable to adapt, providing skills training and emotional support may be effective in mitigating adjustment problems (Kotter & Schlesinger, 2008).

In situations where speed is essential, coercion may be employed to override resistance. However, this approach is extreme and may result in resentment toward management. In summary, management must carefully consider and implement appropriate strategies for managing resistance to change. These strategies may include education, participation, skills training, emotional support, and, in rare cases, coercion. By understanding and addressing the reasons underlying resistance, management can promote a more effective implementation of changes within the organization (Kotter & Schlesinger, 2008).

This discussion of strategies for managing resistance to change can be linked to the implementation of a cyber security culture in an organization. As with any change initiative, a cybersecurity culture may be met with resistance. By identifying the reasons for the resistance, management can develop strategies to mitigate it. Education and skills training can be used to address fears and concerns around cyber security. Participation and emotional support can help foster and promote commitment to the cyber security culture.

2.11 Why motivation is important in change management

Motivation is a crucial force that pulls individuals towards achieving success. In a dynamic and competitive market economy, the level of motivation among employees is an important factor in a company's progress and success. Therefore, it is essential for management to address the critical mission of motivating employees. It is important for companies to motivate their employees and this cannot be stressed enough. Employees who are motivated are more committed to the company's objectives and more likely to take ownership of their job, which increases productivity and results in better results. Motivated employees will also more likely foster a positive work environment, which again leads to greater job satisfaction and employee retention. Furthermore, motivated individuals are to seek out opportunities for growth and development, thereby contributing to the company's continued success (Mascalu & Ciocan, 2016).

Companies who fail to focus employee motivation stand the risk of falling behind competitors in today's fast-paced and continuously changing business environment. Effective leaders are dedicated to fostering a culture that encourages motivation because they recognize the critical role it plays in attaining company goals. Management can guarantee that their staff members are committed to their mission and inspired to meet the organization's objectives by developing a culture of engagement and inspiration (Mascalu & Ciocan, 2016).

Theories of motivation are critical to change management, as they provide insights into the drivers of human behavior and can help guide the implementation of effective strategies to motivate individuals during the change process. Generally, theories of motivation can be categorized into two categories: Intrinsic theories and Extrinsic theories. Behavior motivated by intrinsic factors such as self-expression, interest and enjoyment. And then you have behavior motivated by extrinsic factors such as the promise of a reward or threat of punishment (Clegg, Kornberger, Pitsis, & Mount, 2019). These theories describe the types of needs that must be met to motivate individuals, while process theories help understand the actual ways in which we and others can be motivated. During periods of change, employees might experience a range of different emotions and reactions, such as fear, anxiety, and resistance. Effective change management requires understanding the factors that motivate individuals and how to address any concerns they may have. Leaders must identify the motivators and hygiene factors that drive their employees and create strategies that align with their values and priorities. In addition, leaders must provide their employees with support and resources to ensure that they have the skills and knowledge needed to navigate the changes successfully. Motivation plays a crucial role in change management, and theories of motivation provide valuable insights into how individuals can be motivated to achieve organizational goals. By understanding the factors that drive motivation and addressing employees' concerns during periods of change, leaders can create a culture that fosters engagement, innovation, and high performance (Appelbaum, Profka, Depta, & Petrynski, 2018).

2.12 Summary and theoretical framework

The literature review identifies the different cyber threats that the marine sector may encounter, including ransomware attacks, data breaches, and phishing scams. To develop successful responses, it is crucial to understand the nature of these dangers. Also, a number of significant events that occurred in the marine sector highlight the need for strong cyber security measures. For instance, a 2017 cyberattack on the international shipping firm Maersk cost the company approximately $300 million. The incident showed how important it is for maritime firms to put strong cyber security procedures in place.

Furthermore, following the International Maritime Organization (IMO) recommendations and BIMCO's "The Guidelines on Cyber Security Onboard Ships" can be vital for a maritime organization, according to various studies on cyber security in the maritime industry. They highlight the importance of senior management being involved in creating a culture of cyber risk awareness within the whole organization. In addition, the theory emphasizes the need of spreading knowledge throughout the company and the need for awareness-raising campaigns in order to reduce the human aspect in cyber-attacks. Furthermore, the studies have shown that senior management can employ change tactics based on Kotter's model of change within the business to create a new proactive culture that emphasizes cyber security. This cultural change will not only contribute to reducing potential cyber dangers, but it will also foster a secure and safe work environment.

In conclusion, it is crucial for senior management to lead the way in building a proactive culture that supports security and safety. Organizations can reduce potential risks by incorporating the pertinent rules, raising awareness, putting change management techniques in place, and comprehending the nature of cyber threats.

These are all theories that are relevant when it comes to answering the research questions. The theory is also relevant when it comes to analyzing the interviews and the deductive coding. The theories will be used as a baseline to create categories. (Frankfort-Nachmias, Nachmias, & DeWaard, 2015) The objective of coding is to identify typical patterns of behavior and patterns. (Saldana, 2009) The outcomes are clarified in terms of categories, and these categories are further described through sub-codes. (Marshall & Rossman, 199) Furthermore, Miles and Huberman stated that “Codes are tags or labels for assigning unites of meaning” Codes are usually attached to chucks of varying size. Those might be words, phrases, sentences or even whole paragraphs. (Mils & Huberman, 1994)

Figure 5:Essential elements to reduce risk of cyber-attacks is based on several theories and illustrates the significance of all parts cooperating to mitigate the likelihood of cyber-attacks. The International Maritime Organization emphasizes the importance of cyber risk essential steps and the importance of senior management involvement in implementing these processes within the company. Knotter's theory is based on how a company should operate in order to innovate their company strategy, as well as the significance of empower action and communicating this to them. Boyes and Isbell pointed out, awareness and training are critical because individuals might be the most vulnerable point in any secure system. As a result, cyber security awareness and training are critical in order form employees to know what to look out for.

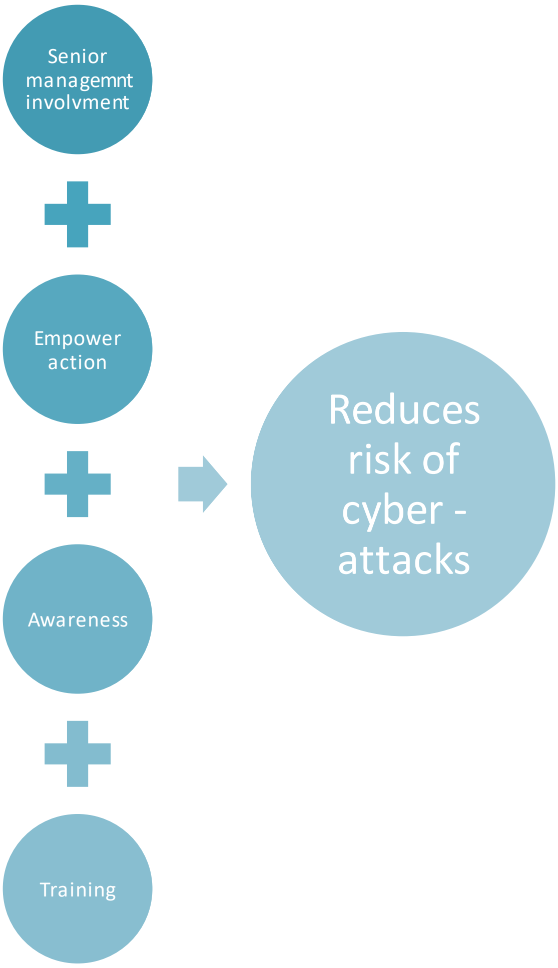

Figure 5: Essential elements to reduce risk of cyber-attacks

Author	Codes	Sub-codes
BIMCO, 2023 Boyes & Isbell, 2017	Cyber Security Definition	Threats, Important
International Maritime Organization, 2017	Senior management involvement	Guidelines
Knotter, 1995	Senior management involvement	Communication
Capano, 2021	Proactive security culture	Consequences
Hopcraft, Tam, Misas, Moara-Nkwe, & Jones, 2022	Proactive security culture	Prevention
Boyes & Isbell, 2017	Training and awareness	Training methods

Table 1: Coding linked to literature

3. Chapter III – METHODOLOGY

3.1 Research methods

This research approach includes two comparative case studies and interviews with Norwegian employees in two shipping lines to better understand their cyber security measures and the impact of human factors as well as cultural and managerial factors in mitigating cyber-attacks. Comparative case studies focus on analysis of the similarities, differences and patterns across two or more cases that share a common mission (Goodrick, 2020).In this study, Company A and Company B are companies that are located in Norway. However, both have headquartered in countries outside of Norway, will be subjected to a case study analysis. Through interviews with personnel from these organizations, the aim is to investigate their cyber security risk mitigation and the human factor in developing a cyber security culture. Furthermore, by contrasting the results from the two case studies, the aim is to identify the strengths and limitations of various cyber security approaches employed within these two maritime companies. By highlighting the human factor within an organization, the study's findings may help design more successful ways for fostering a proactive security culture. Due to constraints in time and resources, the interviews were conducted solely with onshore employees within the two companies.

3.2 Research design

The qualitative design was selected because it aims to study institutions and behavior by learning about the people who are engaged and their values, rituals, beliefs, and emotions. In qualitative research, the goal is to record, summarize, and comprehend the data being gathered (Frankfort-Nachmias, Nachmias, & DeWaard, 2015). Comparative case studies are an appropriate design choice for investigating processes or outcomes of an intervention when the research questions are related to the "how" and "why" aspects (Goodrick, 2020). While case study research employs comparable techniques to naturalistic inquiry, data collecting is often more organized. Key informant interviews and structured observations of events and interactions are the most often employed techniques. Although there are many different types of interviews, the questions usually stay open-ended (Sofaer, 1999). The use of two case studies was found to be the most efficient method for this study as it allowed for the comparison of patterns of observed outcomes across various variables (Bitektine, 2008).

However, there are some limitations and disadvantages when using a qualitative case study design. One of the restraints is that it can be difficult to generalize the findings from a case study to a larger population (Creswell, 2015). This is because the data collected in a case study is often unique to the particular context and participants involved and may not be representative of a larger population. Another limitation is that case studies can be time-consuming and resource intensive (Creswell, 2015).

3.2 Population/sample

The population of this study is the Norwegian maritime shipping companies. The Norwegian maritime industry has developed into an extensive maritime environment, that includes companies across the entire value chain with solid positions in specialized industry sectors. (Regjeringen, 2021) Company A and Company B are both important players in the maritime industry. They offer global transportation and logistics services, and they have a large fleet of ships as well as a global network of offices and agents. Company A and Company B, both have headquarters based in countries other than Norway, will be subjected to a case study analysis. However, interviews with Norwegian employees will take place at the Norwegian office. Each company had one managing director, one sales manager, and three operations customer service employees participate. The 10 participates have the same roles in their respected companies. Based on this it will provide the best results to base the analysis on comparing the companies against each other. However, since the participants have various roles within the company it is also possible to research if this impact their knowledge and behavior regarding cyber security measures. In addition, it is important to point out that company B had two employees with a short career (2 months and 10 months) therefore they might not have the same insight to the cyber security guidelines and had the same training as the rest of the employees at company B.

3.4 Data collection method

The data collection for this research was carried out through a series of in-depth interviews with 10 participants form 2 different companies. Annual reports and relevant internal procedures were also review as a way of gaining more insight to the awareness and focus of cyber security within the companies. The insights gained from the interviews, literature review and internal notes were used to explore the ways in which the companies perceived the issue of cyber security and the steps they were taking to address it within their organizations. In a semi-structured interview, the subjects that must be covered are defined in an interview guide, but there is still some flexibility in the questions that may be asked and the information that can be gathered. This aims to create a balance between the standardized character of a structured interview and the in-depth and an unstructured interview. Additionally, it offers a high level of consistency in the data gathering procedure, guaranteeing that all participants are questioned the same way and that the data gathered can be quickly compared and evaluated (Harrell & Bradley, 2009).

The interviews took place between March 27th and 29th in meeting rooms within the offices of the participating companies. The case study design allowed for an in-depth explanation of the experiences and perspectives of the participants, providing valuable insights into the topic being studied (Bitektine, 2008). The interviewer and participant interacted face-to-face during the semi-structured interview, which was performed in a private meeting room. This strategy was chosen to create a comfortable and informal environment that would enable the participant to share their individual insights and experiences. Face-to-face interactions also give the interviewer the chance to pick up on non-verbal indicators, which can add important details and deepen the information gathered (Sofaer, 1999).

The interview's framework was developed in accordance with the data that was supposed to be gathered regarding organizational vulnerabilities relating to cyber security. There were three sections to the interview. The first section of the interview was "Personal”. In this section there is gathered insight about the employee's job title and length of employment with the organization. Furthermore, if they could explain cyber security and why this is important for the company. The second section was developed to gain more information about "general understanding about cyber security in the firm". The major goal of this part was to determine whether the employees were aware of the company's cyber security policy and whether they believed senior management had taken action to prevent possible cyber-attacks. The goal of the last section, "Training and awareness," was to obtain understanding of how the company ensured that the employees had the necessary knowledge to be able to reduce the risks of a cyberattack. The average length of each interview was estimated to be 20 minutes, but there was some room for flexibility. A collaborator who was unrelated to the study was used to test the interview guide as a pilot before the interview (Bryman, 2012). The interview guide can be found in Appendix I. The interviews were recorded with the intention of processing and analyzing (Frankfort-Nachmias, Nachmias, & DeWaard, 2015).

3.5 Data analysis method

When analyzing a qualitative data set the use of coding is important. Coding is the process by which responses by interviews are classified into meaningful categories (Frankfort-Nachmias, Nachmias, & DeWaard, 2015). This analysis is based on deductive coding the suggested categories is based on theory to fit the specific population (Frankfort-Nachmias, Nachmias, & DeWaard, 2015). Table 1: Coding linked to literature on page 35 illustrates the coding based on literature and the sub-codes. This will make it possible to identify how Company A and Company B views the different challenges and to create patterns. These patterns can again be divided into sub-codes which means more specific codes to get even more details for the data collected from the interviews. The first step of the data analysis is the transcription, which involves close observation of data through carefully repeated and attentive listening, is the initial step in organizing and evaluating talking or verbal data (Widodo & Puji, 2014). The various ideas identified from data will be categorized into distinct categories, which will result in codes from specified concepts and theory based on relationships from categories (Bryman, 2012). Manual coding was employed to enhance control and ownership of the work (Saldana, 2009).

3.6 Reliability and validity

Validity is concerned with the question “Am I measuring what I intend to measure?” (Frankfort-Nachmias, Nachmias, & DeWaard, 2015). However, it is important to ask the right questions that really hit the target as far as the research question is concerned. It is important to be sure that the indicators that is used accurately reflect the concept they are investigating. A large number of the employees' responses were consistent, which established the study's validity and contributed to its credibility.

The quality of the approaches is referred to as reliability. Researchers must be confident that the methods they employ will be consistent and will not generate fluctuating results. They must understand that any variation in results discovered when applying the procedures signifies a genuine difference in the property being tested rather than a rogue' mis-reading' created by an untrustworthy instrument (Denscombe, 2009). The question that was asked in the interviews was clear and with no bias. Furthermore, the sub-codes have been created from common patterns that were identified by multiple participants.

3.7 Ethical consideration

Prior to the initiation of the interviews, a formal agreement was established between the University of South-Eastern Norway and Companies A and B, stating the conditions and specifics of anonymity. Furthermore, the University obtained approval from the NSD (Norwegian Center for Research Data) to ensure the protection of the anonymity of the participants in a legally binding manner. (ref.nr. 332878). The interview subjects, who voluntarily chose to participate, provided their informed consent after being fully informed. The participants gave both oral and written consent before the interview took place, as well as consent for the interview to be recorded, after being fully informed about the purpose and nature of the interview (Frankfort-Nachmias, Nachmias, & DeWaard, 2015).

4. Chapter IV – Findings

The findings of the 10 interviews with participants from Company A and Company B will be obtained in the following chapter. These findings are going to be presented using a descriptive method, which is a methodology that tries to explain or define the subject of the research. In addition, there will also be an explanatory method that investigates the question of why the phenomena occur in the manner in which they do (DeCarlo, 2018). However, the questions are asked in a way that is explanatory, so this will reflect the findings.

4.1 General overview of the case studies

The job position of the participants was divided into 1 manager director in each company, 1 sales manager in each company and 3 operative customer service employees in each company.

Company A employees had an average career within the company of 7 years and 4 months, with the longest employment being 16 years and the shortest being 2 years in a part-time position. The average career in Company B was 3 years and 2 months, with the longest being 8 years and the shortest being 2 months.

Employees from both Companies A and B described what cyber security is and why it is important to the company. They emphasized the necessity of data system security, the protection of private and sensitive information, and the protection from potential cyber-attacks.

4.2 Interview time and environment

The interviews lasted an average of 16.5 minutes, with a minimum of 11 minutes and a maximum of 23 minutes. There could be a variety of reasons for the variation in interview times, such as some participants may give brief, short remarks, while others may go into greater detail. Also, some of the questions are more challenging than others and may have been difficult to answer for some of the participants. This was especially notable in company B with the employees that had only been in the job for 2 and 10 months, and also with the part time employee at company A.

All interviews with participants for Company A were conducted in a private meeting room, as scheduled. Except for one interview, all interviews at Company B were conducted in person. This was due to the participant's was not feeling well, and this interview was conducted via Teams. The remaining interviews were also conducted in a private meeting room.

4.3 General knowledge about cyber security in the company – Company A

The employees at Company A points out that cyber security is an important issue to be aware of and try to mitigate. In addition, it is clear that the information they receive considering cyber security is via intranet or the IT department. When it comes to creating a proactive cyber security culture, they have onboarding and the possibility to reach out to the IT department. It has also been implemented some protective measures such as VPN and multi-factor authentication. Throughout this chapter we will look into the interviews via transcripts and a general summary of the interviews with company A. The finding will be divided into two parts: “General knowledge about cyber security in the company” and “Training and awareness”. In addition, there will be a table illustrating the section of the interviews, code, sub-code and extracts for transcripts. There will also be some transcripts outside of the table.

Section	Code	Sub-code	Extracts from transcripts

Personal	Cyber Security Definition	Threats:	“*Cyber security is the protection of the company's files as well as all the information that is gather both from customer as well as the carrier. The reason why it is very important to protect the information is because some of the information is sensitive and could break the chain of supply*"
		Importance:	“*I think it's important for companies to be prepared if there's something, and I think it's more cyber-attacks than earlier because everything is more technical now*”
General knowledge about cyber security in the company	Senior management involvement	Guidelines:	“*I know that there are some guidelines on the intranet, but I’m not really there often, I should probably check in more often*”
		Prevention:	“*We have a multi-factor authentication for all our devices, meaning we not only need to import the password, but we also need to input the password together with a code that we get on our cell phone whenever we try to log into the system from an internet outside of the office*”
		Communication:	“*We have done small steps, but of course a lot of things happen behind the scenes that we are not aware of*”
	Proactive security culture	Consequences:	“*Well, an unwanted attack is something that happened to our competitor a few years ago. I remember their systems*

			went down for several days, that means customers won't get their bookings and customers won't get their arrival notice, the system just completely stops”
Training and awareness	Training methods	Onboarding:	“*When you start the job, you need to go through an onboarding program where you have courses about GDPR to cyber security*”
		Frequency:	“*We have not had any cyber security training to last year, but we have gotten some updates by e-mail and on our intranet*”
		Compliance:	“*A mandatory course you have to take online when you started in the company, that's it*”
		Prioritization:	“*Yes, I do think so. I think it is important these days and you can see other companies in our business that has been hacked*”

Table 2: Coding linked to literature – Company A

When it comes to general knowledge about cyber security, Company A states that they receive updates via email, but not all of them are aware of the company's cyber security guidelines. “*I don't actually have a lot of knowledge about it. But I do get some emails from time to time regarding updates and what not to click on when it comes to emails and suspicious links, but other than that I don't really have much insight into the cyber security policies in the organization*” However, other employees were well aware of the company's guidelines. The difference when it comes to this topic can be explained with different roles within the company or how long the employees has been working there. Nevertheless, it is important that ever single employee in the company have knowledge about cyber security guidelines and knows how to act in case of a cyber-attack.

When being asked about the potential consequences of an unwanted cyber-attack, all of the employees at Company A, with the exception of the manager director, mentioned the prospect of private and sensitive data getting out. "*Private and sensitive data being visible for both our competitors and other people that should not have access to that information*". However, the manager director pointed out the possibility of a shutdown in the business of it got hacked. "*Well, we could have a complete shutdown for an unknown period. We have seen before that competitors had it for like 3 weeks and there was nothing to do actually. We could close the door and lose a lot of revenue internally*". This could be explained in different objectives when it comes to this issue. The manager director might have a more financial approach than the other employees.

It's also been mentioned that phishing emails are the most dangerous type of cyber-attack, although IT is doing an excellent job of preventing suspicious emails. "*We don't deal with the IT. The proper IT protection of the system form Norway it is mostly screening emails and making sure that you do not open those questionable links and we have a good IT department that helps with identifying these for us*". Three out of every five employees at Company A reported that they did not have the perception that their organization has a proactive culture regarding cyber security. However, the part-time employee in customer service, it can be defined a proactive culture as such "*I would define proactive security culture on how we as an organization prevent unwanted incidents before they happen. I know that there haven't been any cyber-attacks on our company that have caused us any trouble, but I don't feel like I have gotten a lot of information when it comes to cyber security*".

Regarding the question of if they knew anything about measures senior management had implemented any procedures to identify and minimize the potential risks, two out of five stated that they had not received any information regarding this matter. Nevertheless, the three other workers stated that there were several precautions taken, but that the IT department was the only one that communicated information regarding the company's cyber security. "*We have multifactor identification login system and we also use programs that are pretty resistant regarding phishing and malware such as java script and also personal passwords and one-time password that gets send to our phone every morning when we log in, so you need to have a lot of information to be able to login to someone's user ID. We also use VPN both at home and in the office, and the rules from the IT department are continuously being updated*".

4.4 Training and awareness – Company A

Company A has cyber security awareness as a part of the companies onboarding program and the manager director states very clearly that everyone have to complete this program. "*Yes, yes yes of course. They even must sign a contract on what to do and not to do and then they have to confirm that they have read it*". However, not all of the employees have got the cyber security onboarding program. The part time customer service employee said that he has not had any onboarding program when it comes to cyber security. "*Yes, however I have not gotten any*". This can be explained due to the fact that the part time employee only works a couple of days a week. However, it is important for company A to make sure that all of the employees receive the onboarding to create awareness and knowledge about cyber security threats.

Only one of the employees have had any training about cyber security the last year. So, if this have been a miscommunication or if everybody else just missed it is unsure. However, when it comes to making sure that employees understand and follow security policies and procedures the answers were mixed and some of the employees pointed out the emails and information on the intranet. The intranet was also pointed out as a place where the employees could find more information about cyber security as well as contacting the IT department. IT is also highlighted when discussing the sufficient actions that senior management has taken to strengthen the cyber security training and awareness. It is very evident that every worker at company A is under the impression that senior management has taken actions to improve training and awareness, despite the fact that this information is provided through the IT department. "*I know that the IT department sends out some emails from time to time, and I guess this on behalf of senior management, but other than that I don't know*". One of the

employees also pointed out IT might not be your area of expertise as a senior manager. "*I do believe that was a senior management decision to delegated this to people who know more than them. I think that's the best we can say about senior management contributed because their IT competence might not be that high. We are talking about older people here and of course they have an IT department that's on top of things and follow up on things".*
When it comes to matters of cyber security IT have better insight to these issues than senior management. This could be one of the reasons why the IT department oversees the communication of the measures that are being implemented.

When it comes to if the company should prioritize cyber security training and awareness more there are some different opinions. Three out of the five employees believe that this is important and something that needs to be in focus. "*Yes, I do think so. I think it is important these days and you can see other companies in our business that has been hacked*" However, the two remaining employees believes that the training is prioritized enough, and that cyber security awareness is well implemented in their everyday routine. There could be several reasons why this matter is perceived different for these two employees. They might have more meeting where cyber security is talked about or they might have a more personal interest in the subject. However, all the employees managed to point out things to be aware of when it comes to phishing emails.

4.5 General knowledge about cyber security in the company – Company B

The employees at Company B said that cyber security is important because the consequences of a cyber-attack can be critical for the company. They point out that they might lose sensitive information and the company might have to shut down all activity in a period. In addition, they point out that cyber security is an important issue to be aware of. Company B have onboarding training for all the employees and they also have yearly mandatory cyber security training. In addition, just as Company A they have implemented preventing measures such as VPN and multi-factor authentication. This section is divided in the same way as the findings for company A. In the end of this chapter there will be a summary of similarities and differences between the measures that is implemented by both companies.

Section	Code	Sub-code	Extracts from transcripts
Personal	Cyber Security Definition	Threats:	"*Cyber security from my point of view is that the security system that a company has to protect itself from being hacked works*"
		Importance:	"*This is important in order to avoid cyber-attacks such as ransom and phishing attempts*"
General knowledge about cyber security in the company	Senior management involvement	Guidelines:	"*In the training courses that we do, we get knowledge about how to detect and identify potential phishing and malware attacks. It's also a lot of focus on being cautious, aware and report if you get any emails that looks suspicious*"
		Prevention:	"*We have the two-phase authentication se we have to either use an app or get the code sent to our cell phone. We also need to use VPN if we are outside of the office*"
		Communication:	"*We are taking cyber security very seriously, however I don't know all of the details because this is really related to IT and they are following all of the security threats closely. They only*

			communicate if there are any specific threats that we need to be aware of”
	Proactive security culture	Consequences:	“*We could lose sensitive information both our own and our customers. This would lead to a shutdown of the entire system, and we wouldn’t be able to provide our customers with information about when their cargo will arrive or where their cargo is at this time*”
Training and awareness	Training methods	Onboarding:	“*Every new employee has to go through the mandatory training that we have about cyber security*”
		Frequency:	“*Yes, we have a cyber security training session in the beginning of every year*”
		Compliance:	“*If a threat is occurring, we will receive an E-mail from our IT department regarding this. We will then follow up with a daily discussion in the office regarding this issue and what to be aware of. I believe this helps to keep the awareness*”
		Prioritization:	“*I think it depends on which country you are working in. I think in Norway we a have a good awareness and we know what kind of links that we should not click on”*

Table 3: Coding linked to literature – Company B

Regarding Company B, it is notable that they receive their cyber security policies and knowledge through email and training programs in their own academy. “*We get information* *about the policies within the training program, and we also get some emails if there's anything that we need to be aware of*". When it comes to consequences of an unwanted cyber-attack, Company B mention loss of sensitive information and how this could lead to a shutdown of the company in a period of time. It is also pointed out that this could lead to a financial loss. "*We could get sensitive information going around and this could result in losing customers, losing business and a lot of financial loss*". In Company B phishing emails with malware is pointed out to be the most threatening because some of them are quite sophisticated. They have also been a victim of this type of cyber-attack a couple of years ago. However, after this attack the company implemented some new measures to avoid this from happening again. "*I think phishing emails are the most threatening. It might be hard to spot and it can do a lot of damage. We have this phishing alert that you can press as soon as you have a suspect e-mail".*

Company B has implemented a multifactor identification login system as a preventive measure against cyber-attacks. Another measure that has been implemented is a program similar to VPN, which must be connected prior to logging into any Wi-Fi network outside of the office. The importance of attentiveness when it comes to unknown emails and avoiding clicking on any links has been pointed out, along with the clear guidelines to identify suspicious emails. "*We as employees in the company need to be proactive and be aware if there's some suspect e-mail for example coming into our office. We are more or less told that we should never click a link for example which is coming from a party which seems suspect, or we should also always check the e-mail addresses if it's really the real person we have contact with them. In general, we have to be very careful and about how we treat emails and the same goes with protocols, and with someone would call us and ask for a company account number or something like that. We would immediately not give any information but instead hang up trying to ask for the name and the number of the person*".

Regarding the question of whether they knew anything about if senior management had implemented any procedures to identify and minimize the potential risks, 4 out of five said that they believed that senior management had implemented procedures. They pointed out procedures such as multifactor identification login system, VPN and phishing alerts. However, in company B the exact measures and the importance of this might not have been communicated to the employees. "*I think that we as a company are taking security measures all the time. I don't know details about it because it was like very much IT related matters but I'm already following it closely and we are on the high security level the company. I think it's hard for me to give an example on this subject as this one part of my daily job*."

4.6 Training and awareness – Company B

All of the employees at company B stated that they participated in an onboarding program when they first started in the company. All of them also said that they have received cyber security training within this year. However, it is essential to highlight the fact that two of the employees have been with the organization for less than a year. Therefore, the onboarding program and the training program for cyber security will be combined into a single training program. When it comes to the methods by which the company ensures that employees understand and follow the organization's security rules and procedures, Company B has a few different points of view. It is mentioned that they experienced a cyber-attack a few years ago, and as a result, they had to adjust the way that they operated. It involves a higher priority on training, presenting the various outcomes that could result from an attack, and raising overall awareness in the workplace. "*That's a good question, I think the main driver is to get training that we do and having the IT following that up on a regular basis towards us so if anything would happen. Even if it's a small thing that would be like an internal distribution about this this issue that has occurred and also to follow that up the daily discussions in the in the office would also help yeah to keep the awareness about it*."

The employees at company B points out that the information about cyber security is available at the intranet and that they also have the IT department they can ask if they have any question, or if they want to learn something more about the topic. The employees of Company B say that senior management have implemented measures, after the cyber-attack they had a couple of years ago. They have got stricter rules and guidelines and cyber security awareness is a really high priority within the company. However, these need guidelines have been communicated through the IT department.

There currently exist different opinions within Company B regarding the degree of focus that should be placed on prioritizing cyber security training and awareness. Several employees expressed their opinion to increase the cyber security training to be able to keep up with the current cyber threats. However, other employees pointed out that they feel the yearly training is enough and that relevant cyber threats gets discuss in the office. Additionally, it has been suggested that in Norway, there exists adequate training to effectively address this issue. "*I think that it depends on which country you are working in and I think in Norway we have all the necessary training and are well aware*."

4.7 Similarities and differences

Both company A and company B receive their guidelines and policies through the intranets of their individual companies. Furthermore, both companies receive emails informing them of current cyber threats that they need to be aware. The workers all agreed that the IT department was the one that provided information relating to cyber security. As a result of this, it appears as though this may be standard procedure for the sector, and this could possibly be deemed the greatest technique for employees to acquire information on cyber security related requirements.

All of the employees at both company A and Company B agree that phishing emails are potentially the most dangerous type of cyberattack that might be launched against the company. An explanation for why this vulnerability was pointed out by everyone might have to due to the fact that a number of maritime companies included Company B have been victims of this type of hacking in past years.

In addition to the fact that there are a lot of similarities, there are also a few differences when it comes to the way in which they focus on concerns connected to cyber security. Company A stated that they were required to have training once each year, however, it appears that not all of them had participated in this training. When it comes to firm B, each of its five employees has completed the annual training, and the instruction on how to protect company data from cyber-attacks took place at the beginning of the year. There were also other distinctions that might be discovered in the yearly report. Company A included a chapter about security, as well as several paragraphs about cyber security and the safety measures they have put in place. Company B, however, did not include anything at all regarding cyber security, and they did not address it in their annual report until the year that they were the target of a cyberattack. In the years after the attack, they did not add any information regarding measures they had put into place.

5. Chapter V - Discussion

This research investigated the importance of different aspects of the human factor and organization culture when it comes to mitigate cyber-attacks within a maritime organization. Furthermore, what kind of measures Norwegian maritime companies currently have implemented to mitigate the risk of cyber-attacks and increase the cyber security awareness within the company. Cyber-attacks in the maritime industry have increased a lot the last couple of years, therefore it is important to be proactive when it comes to this issue. (Kechagias, Chatzistelios, Papadopoulos, & Apostolou, 2022) In this chapter we will connect the answers form the interviews with the theory from previous research and the research questions.

RQ1: What mitigating actions have been implemented by the two Norwegian shipping companies to prevent successful cyber-attacks?

5.1 Guidelines in day-to-day work

Guidelines regarding maritime cyber risk management could be a useful tool for companies to implement to raise awareness. This can help the employees focus more on cyber security and in this way mitigate the risk of cyber-attacks. The internal guidelines of both companies are posted on the intranet, however the issue with this is that not everyone uses the intranet actively, and therefore they will not read these guidelines. As a result, not all of the employees are aware of what kind of guidelines they need to follow when it comes to cyber security. To solve this issue senior management could designate a person in every single office to take responsibly to pass on all relevant information related to cyber security. To create a “cyber security champion” can be beneficial to make sure that all of the employees reads the guidelines and reads the updates on current threats or issues.

5.2 Multi-factor authentication

7 of the 10 participants in this study pointed out that their company had implemented Multi-factor authentication. This is a security measure that requires two or more steps to prove you identify to give you access to the devise, files or other valuable information. (Australian Government, 2023) The multi-factor authentication can be linked to the second stage in the guidelines form IMO which is “Protect”. A multi-factor authentication can help the companies protect their systems from a cyber-attack. The manager director in company A has also got feedback from the IT department that this has stopped several potential attacks. However, it is important to point out that the effectiveness of any security measures cannot be guaranteed and that it is very important that companies continue to focus on this issue. Nevertheless, multi-factor authentication is a step towards strengthening cyber security in the companies. -

5.3 VPN

VPN is a Virtual Private Network and it as an encrypted connection over the internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. (Moskowitz, 1997) It is also pointed out by participants in both company A and B that VPN or another system with the same qualities is mandatory to use. This highlights the importance placed on this security measure in companies. VPN can also be linked to the “Protect” stage in IMO’s guidelines. As this also works in a way that can help companies avoid cyber-attacks. However, VPN is a tool that needs to be logged into every single time the computer is turned on. Therefore, also when it comes to VPN a “cyber security ambassador” could be a useful because they can remind everyone in their office to always login to VPN. –

5.4 Summary

Overall, we can see that the two maritime companies have implemented various cyber security guidelines and mitigating actions to improve their defense. However, if the companies fail to enforce and ensure understanding and compliance with these guidelines, their existence will not add value to the company and its defense. To address this, companies should give extra responsibility to "cyber security champions" to make sure that the guidelines are been communicated to all the employees in the office. During interviews, the technologies of multi-factor authentication and virtual private networks (VPN) are brought up the most. By prioritizing these measures and fostering a culture of cyber risk awareness, these companies aim to mitigate potential threats and safeguard their operations.

RQ2: What does onshore employees in the two maritime companies in Norway do to improve their cyber security awareness?

5.5 Training and awareness

IMO has stated that one of the main challenges to improve cyber security in the maritime industry is the lack of awareness and training among the employees in the industry. (International Maritime Organization, 2017) Research also shows that maritime industry has the framework, however it is not a priority. (Cyber Risk GmbH , 2020) As the human factor is one of the biggest vulnerabilities when it comes to cyber-attacks it is critical for companies to prioritize training and awareness. Low awareness is also named the first vulnerable point of the industry regarding cyber security. (Cimpean, et al., 2011) According to company A and B is training already implemented as a measure to improve their cyber security awareness. However, only company B have had their yearly training. Some of the employees felt that having more than one mandatory training a year would be too much. Nevertheless, some of the same employees did not have an overview of where they could find company guidelines regarding this issue. Based on this it can be valuable to have shorter sessions on a more regular basis to raise awareness. It could also be useful with some mandatory tests to check if the employees understood the training and are about to use the knowledge in a practical matter. In the annual report from 2020 from company A they state several measures that they have implemented to mitigate the risk of cyber-attacks. A number of these measures are associated with training in order to raise the awareness within the company. However, company B do not have information regarding measures they have implemented in regard to this issue. Nevertheless, they inform that they have been a victim of a cyber-attack.

5.6 Knowledge

In order to gain and improve knowledge training an important tool. The training that is being provided should give the employees insight into the current state of cyber security in the maritime industry, and knowledge of the types of threats that can occur. Everyone participating in the interview were able to mention three check points in identifying phishing attacks. It is also stated that they receive emails form the IT department with information about things to be aware of and to always reach out if they have any questions or concerns.

5.7 Culture

It is important that they have the right knowledge, training and sponsorship from senior management to create a proactive cyber security culture. In both of the companies the employees have split opinions when it comes to culture some say that they believe that the company have a proactive cyber security culture, while other do not. To tackle this issue senior management, needs to prioritize education and training to address insecurities regarding cyber security.

5.8 Summary

The two Norwegian maritime companies in this study work to increase their cyber security through training and awareness initiatives, improve knowledge about cyber security threats and creating a proactive cyber security culture. Even though they have a way to go regarding creating a proactive security culture were all of the employees are well informed and receive training on a regular basis.

RQ3: How does the two maritime companies create a culture that emphasis cyber security awareness and training?

5.9 Onboarding

Two of the most common reasons of human error is unfamiliarity and understanding. (Khripunov, 2023) Based on this information an onboarding program with focus on cyber security could mitigate the risk of human mistake because the new employees get familiar with the different threats and they get an understanding of why this is important.

In both company A and B cyber security awareness and training was a part of the companies onboarding program. This was a program that was mandatory in each company. However, in company A the part time employee had not done the onboard training. This could be critical for the company because it is important that everyone working in the system get this onboarding to increase their awareness. Boys and Isbell stated the also stated the importance of training as a part of their introduction to all employees even if they were temporary staff or agency workers. (Boyes & Isbell, 2017)

5.10 Intranet and emails

A lot of the communication regarding cyber security is distributed to the employees via E-mails and posted on the intranet. When posting company policies and guidelines on the intranet without checking to see if employees really read them is that it increases the possibility that a significant number of employees are unfamiliar about the guidelines. As a result of this, it might be useful to have a “cyber security champion” in each office who is responsible for informing about new rules or regulations and making sure that everyone reads it. A cyber security champion would be responsible for bringing up the content of the e-mails and articles posted on the intranet. The champion would make sure that every employee understood the content, and this could help create understanding and ownership when it comes to cyber security.

5.11 Yearly training

Some employees at Company A say that they have yearly training, while others don't. Therefore, Company A need to implement mandatory yearly training and make sure that everyone performs the training. In Company B all of the employees stated that they have yearly cyber security training. In order to make the employees pay better attention to the training a mandatory test should be at the end. In addition, sending out a fake phishing mail could also be a tool to create awareness. All of the employees that click on the link or do not understand that this is a phishing e-mail need to take a new course in cyber security. In this way the employees will be more alert and on the lookout for suspicious emails.

5.12 Summary

The importance of creating a company culture with focus on cyber security is a serious mission and should therefore be a priority for the companies. There is currently a high focus on the cyber security onboarding program that will help to new employees gain knowledge regarding the current situation and threats they need to be aware of. However, a lot of information regarding cyber security is distributed to the employees via emails and intranet Therefore, some of the employees do not get this information. The companies also have a yearly cyber security training. Nevertheless, not all of the employees in company A have had any yearly training in the last year even though this is mandatory.

RQ:4 How does senior management work to play a more active role in creating and carrying out cyber safety measures?

5.13 Senior management need to communicate and empower action

According to various literature the involvement and importance of a senior manager leading the way when it comes to carrying out the cyber security measures can be critical. They need to create a vision together with help from the IT department and communicate this vision to the whole organization. They need to emphasis the importance of this issue and empower action to the employees. However, both in Company A and B there is a lack of communication regarding this issue form the senior management side. Without clear and consistent communication from senior management, employees may not fully understand the significance of cyber security measures or may not prioritize them appropriately. The involvement and commitment of senior management are critical for ensuring that cyber security measures are implemented effectively and that employees are trained and supported in their use. When it comes to company A their annual report from 2021 states some of the measures the participants mention in the interviews, however there is a lot more measures they have implemented without communication this to the employees. Some of the resources they have implemented to help detect and mitigate cyber-attacks are E-mail anti-blocking mechanism and Unauthorized software installation detection.

The goal of cyber security is to protect the company, the employees and the other stakeholders. The IT department is involved in every decision when it comes to cyber security and what kind of measures that should be implemented. IT has first-hand knowledge about this issue, and they should always be updated on the current threats. Company A and B both pointed out that they have good faith in their IT department and the work that they do. However, it is also clear that the IT department is the one that is communication the information as well. However, it is important to note that senior management plays a critical role in creating and carrying out cyber security safety measures. Senior management sets the tone, and they are responsible of allocating resources and budget to maintain and evolve cyber security initiatives.

5.14 Summary

Senior management must prioritize cyber safety measures and communicate the importance of this to the employees. They should ensure that employees receive regular training and updates on cyber security risks and best practices. It is also impornat that communicate what measures they have impemented why it is important that the company as a whole have knowledge of what risks they might be facing and the seriucness of a possible cyber-attack. However, it seems like this is not the case in both company A and B. In both companies all of the cyber security information, guidelines and strategy is communicated via the IT department.

5.15 Limitations

The study's methodology has a few limitations. The content may be constrained and may not represent the entire range of experiences or opinions relating to the subject matter because these two companies are fairly small. This can effect the credebility of the study. Futhermore, the only employees included in this study are those who work in the Norwegian office, employees who work abroad or aboard ships are not taken into consideration. Additionally, the likelihood of bias in the responses exists. It's likely that the participants felt under pressure to provide specific responses due to the nature of the survey or their relationship with their company. The fact that it is challenging to keep the identity of the participants and companies confidential throughout the research is another drawback of this study. Therefore, is was made some small changes to the transcript in some places. Additionally, all of the interviews were conducted in English. Both the person conducting the interview and the participant were non-native English speakers. Despite this, both the interviewer and the participants have a lot of expertise using the English language in their respective industries. This situation has the potential to cause confusion or misunderstanding, but this obstacle has been addressed because both the question and the response provide an explanation of the concepts.

6. Chapter VI - Conclusion

It is important for maritime companies to implement a multi-layered cyber security approach. The cyber-attacks toward the maritime industry have increased in the recent years, so this issue needs to be prioritized as a cyber-attack could cost a company millions of dollars. Through the insight gained from the interviews it is clear that these two maritime companies take this issue seriously. They have implemented measures such as VPN and multi-factor authentication as a prevention tool against cyber-attacks. Both companies also have an onboarding program and a hands-on IT department that posts information about current threats. In both companies the employees have faith in senior management when it comes to measures, they have implemented regarding cyber security. However, it is clear that in both companies' senior management need to take a more active role in communicating the importance of cyber security. In addition, previous literature focus on the importance of creating a proactive cyber security culture. Senior management must take an active part in creating and communicating this to the employees. In addition, a "cyber security champion" was suggested as a measure that could increase the awareness and understanding within the companies. In conclusion, this study found that cyber security is taken seriously with the two maritime companies. However, they still have a way to go in order to create a proactive cyber security culture.

6.1 Future studies

Due to the fact that this study is based on two maritime companies, it is possible to conduct future research comparing the findings with Norwegian and foreign companies. It is also possible to conduct quantitative research to generate more responses and obtain a broader perspective from participants in a variety of industry positions. In addition, future research could investigate new technologies such as artificial intelligence and blockchain to determine how they could be utilized to enhance cyber security in the maritime industry.

However, future research could also examine the efficacy of various training methods and technologies, such as gamification and virtual reality training, in enhancing employee cyber security awareness and preparedness.

Bibliography

Appelbaum, S., Profka, E., Depta, A., & Petrynski, B. (2018). Impact of business model change on organizational success. *Industrial and Commercial Training*, 50(2), 41-54.

Australian Government. (2023, April 29). *https://www.cyber.gov.au*. Retrieved from cyber.gov.au/protect-yourself/securing-your-accounts: https://www.cyber.gov.au/protect-yourself/securing-your-accounts/multi-factor-authentication

Bateman, T. (2013, October 16). *bbc.com*. Retrieved from https://www.bbc.com/news: https://www.bbc.com/news/world-europe-24539417

BIMCO. (2021). *IMO.ORG*. Retrieved from https://wwwcdn.imo.org/localresources: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ANNEX%20Guidelines%20on%20Cyber%20Security%20Onboard%20Ships%20v.4.pdf

Bitektine, A. (2008). Prospective Case Study Design: Qualitative Method for Deductive Theory Testing. *Organizational Research Methods, 11(1)*, 160-180.

Blum, D. (2020). *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment.* New York: Springer Science.

Bolman, L. G., & Deal, T. E. (2017). *Reframing orgnizations 6th edition.* Hoboken, New Jersey: Jossey-Bass.

Boyes, H., & Isbell, R. (2017). *Code of Practice Cyber Security for Ships.* London: Institution of Engineering and Technology.

Bryman, A. (2012). *Social research methods (4th ed.).* Oxford: Oxford University Press.

Capano, D. E. (2021, September 30). *www.industrialcybersecuritypulse.com*. Retrieved from www.industrialcybersecuritypulse.com/threats-vulnerabilities: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/

Cimpean, D., Meire, J., Bouckaert, V., Casteele, S. V., Pelle, A., & Hellebooge, L. (2011). *Analysis of cyber security aspects in the maritime sector.* European Network and Information Security Agency.

Clegg, S., Kornberger, M., Pitsis, T., & Mount, M. (2019). *Managing & Organizations: An introduction to Theory and Practice.* London: SAGE Publications Ltd.

Corradini, I., & Nardelli, E. (2019). Social Engineering and the Value of Data: The Need of Specific Awareness Programs. In T. Ahram, & W. Karwowski, *Advances in Human Factors in Cybersecurity* (pp. 69 -75). Washington D.C.,: Springer.

Creswell, J. W. (2015). *A Concise Introduction to Mixed Methods Research.* Los Angeles: SAGE.

Cyber Risk GmbH . (2020, December 1). *maritime-cybersecurity.com*. Retrieved from maritime-cybersecurity.com/National_Maritime_Cybersecurity_Plan: https://www.maritime-cybersecurity.com/National_Maritime_Cybersecurity_Plan.html

DeCarlo, D. M. (2018, April 24). *https://pressbooks.pub/.* Retrieved from pressbooks.pub/scientificinquiryinsocialwork: https://pressbooks.pub/scientificinquiryinsocialwork/chapter/7-1-types-of-research/

Denscombe, M. (2009). *Ground Rules for Social Research.* Berkshire: McGraw-Hill Education.

Densker, C., Fortman, F., Ostendrop, M. C., & Hahn, A. (2014). Assessing the Fitness of Information Supply and Demand during User Interface Design. *Proceedings of the 5th International Conference on Applied Human Factors and Ergonomics AHFE 2*, 1-11.

DNV. (2023, May 2). *https://www.dnv.com/.* Retrieved from www.dnv.com/maritime/insights/topics/maritime-cyber-security: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/owners-and-managers.html

DNV. (2023, January 25). *https://www.dnv.com/maritime/insights*. Retrieved from https://www.dnv.com: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html

Frankfort-Nachmias, C., Nachmias, D., & DeWaard, J. (2015). *Reseach methods in the social science - Eighth edition.* New York: Worth Publishers.

Goodrick, D. (2020). *Comparative case studies.* Thousand Oaks: SAGE Publications Ltd.

Graham, L. (2017, February 1). *cnbc.com*. Retrieved from www.cnbc.com/2017/02/01/: https://www.cnbc.com/2017/02/01/shipping-industry-vulnerable-to-cyber-attacks-and-gps-jamming.html

Harrell, M., & Bradley, M. (2009). *Data collection methods : Semi-structured interviews and focus groups.* Santa Monica: Rand Corporation.

Hopcraft, R., Tam, K., Misas, J., Moara-Nkwe, K., & Jones, K. (2022). Developing a maritime cyber safety culture: Improving safety of operations. *Maritime Technology and Research* , 1-18.

IBM. (2023, March 18). *www.ibm.com*. Retrieved from www.ibm.com/topics/cybersecurity: https://www.ibm.com/topics/cybersecurity

International Chamber of Shipping . (2023, January 21). *ics-shpping.org*. Retrieved from www.ics-shipping.org/explaining/: https://www.ics-shipping.org/explaining/

International Maritime Organization. (2017). *GUIDELINES ON MARITIME CYBER RISK MANAGEMENT*. London: International Maritime Organization.

International Trade Administration. (2022, September 12). *Norway - Country Commercial Guide*. Retrieved from https://www.trade.gov: https://www.trade.gov/country-commercial-guides/norway-shipping-maritime-equipment-services

Jones, M. (2017, October 11). *gpsworld.com*. Retrieved from www.gpsworld.com: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/

Kaspersky Lab. (2013). *https://media.kaspersky.com*. Retrieved from https://media.kaspersky.com/en/: https://media.kaspersky.com/en/icefog-apt-threat.pdf

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, 1-14.

Khripunov, I. (2023). *Human Factor in Nuclear Security: Establishing and Optimizing Security Culture.* Cham: Springer International Publishing AG.

Kotter, J. (1995). Leading change - Why transformation efforts fail. *Harvard Business Review*, 59-67.

Kotter, J., & Schlesinger, L. (2008). Choosing Strategies for Change. *Harvard Business Review* , 130-139.

Lagouvardou, S. (2018). *Maritime Cyber Security: concepts, problems and models.* Kongens Lyngby: DTU Technical University of Denmark.

Leite, D., Padilha, M., & Cecatti, J. (2019). Approaching literature review for academic purposes: The Literature Review Checklist. *Clinics (São Paulo, Brazil)*, 1-8.

Lo, C. (2019, April 19). *www.ship-technology.com*. Retrieved from www.ship-technology.com/features: https://www.ship-technology.com/features/ship-navigation-risks/

Marine Digital. (2023, March 19). *Marine-Digital.com*. Retrieved from marine-digital.com/cybersecurity_in_shipping_and_ports: https://marine-digital.com/cybersecurity_in_shipping_and_ports

Marshall, C., & Rossman, G. (199). Designing Qualitative Research. *The Modern Language Journal*, 224.

Martin, K., & Hopcraft, R. (2020). Why ships are so vulnerable to cyberattacks. *Logistics and Transport Focus, 22(8)*, 52.

Mascalu, E., & Ciocan, F. (2016). Attracting and motivation employees during changes in organization. The role of the human resources department. *Journal of Defense Resources Management,* 7(2),153.

Mayberry, M. (2023). *Culture is the way : how leaders at every level build an organization for speed, impact, and excellence.* Hoboken, New Jersey.: John Wiley & Sons, Inc.

Mils, M. B., & Huberman, M. A. (1994). *An Expanded sourcebook - Qualitative Data Analysis 2th Edt.* Thousand Oaks: SAGE Publications.

Moskowitz, R. (1997). What is a Virtual Private Network? *Network Computing Online,* 1-2.

Mottl, C. (2022, March 3). *CoreTech.us*. Retrieved from CoreTech.us: https://www.coretech.us/blog/6-motivations-of-cyber-criminals

National Cyber Security Centre. (2023, January 23). *www.ncsc.gov.uk*. Retrieved from www.ncsc.gov.uk/about.ncsc: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

Norwegian Maritime Authority. (2022, January 20). *sdir.no*. Retrieved from sdir.no/en/shipping/maritime-future/: https://www.sdir.no/en/shipping/maritime-future/maritime-cyber-security/

Regjeringen. (2021, 10 14). *https://www.regjeringen.no/.* Retrieved from https://www.regjeringen.no/no/tema/naringsliv/: https://www.regjeringen.no/no/tema/naringsliv/maritim-naring/ny-temaside/forste-kolonne/maritime-naringer/id2589227/

Saldana, J. (2009). *The Coding Manual for Qualitative Researchers.* London: SAGE Publications Ltd.

Schultz, D. E. (2005). The human factor in security. *Computers & Security,* 24, 425-426.

Sofaer, S. (1999). Qualitative methods: what are they and why use them? . *HSR: Health Services Research,* 34(5 Pt 2), 1101-1118.

The European Parliament. (2018). Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. *Official Journal of the European Union,* 1-60.

The ISACA/CMMI Institute. (2022, February 25). *Narrowing the culture gap for better business results.* Retrieved from www.isaca.org: https://www.isaca.org/-/media/info/cybersecurity-culture-report/index.html

United Nations Conference on Trade and Development. (2020, November 12). *unctad.org*. Retrieved from unctad.org/webflyer/review-maritime-tr ansport-2020: https://unctad.org/webflyer/review-maritime-tr ansport-2020

Watkins, M. D. (2013, May 15). *hbr.org*. Retrieved from hbr.org/2013/05/what-is-organizational-culture: https://hbr.org/2013/05/what-is-organizational-culture

Widodo, & Puji, H. (2014). METHODOLOGICAL CONSIDERATIONS IN INTERVIEW DATA TRANSCRIPTION. *International Journal of Innovation in English Language Vo.l3 Iss. 1*, 101-111.

Appendix I.

Interview guide

Personal

1. What is your job title?
2. How long have you been working in the company?
3. Can you explain what cyber security is and why it’s important for the company?

General knowledge about cyber security in the company

4. Do you have any knowledge of cyber security polices within the company? If yes, how did you acquire this knowledge?
5. What could be the consequences of an unwanted cyber-attack? And how does this affect your department?
6. What do you and your department do to prevent such attacks and have you received any guidelines on how you should work to prevent such attacks?
7. How would you define a proactive security culture? And would you say that the company have been able to create such a culture?
8. What kind of cyber-attacks do you believe are most threatening to your company and why?
9. Do you know about any measures that senior management have implemented to identify and mitigate the potential risks?

Training and awareness

10. Is cyber security awareness a part of the companies onboarding program?
11. Have you had any training about cyber security the last year?
12. How does the company ensure that employees understand and follow security policies and procedures?
13. What resources are available to employees who want to learn more about cyber security?

14. Considering IMO's recommendation that senior management should lead the development and implementation of cyber security initiatives, do you believe that senior management in your company has taken sufficient steps to improve the training and awareness of cyber security among employees?

15. Do you believe that the company should prioritize cyber security training and awareness more?
16. Is there anything else you would like to add to this interview?
17. Could you give me three tips on how to recognize phishing attempt?

Appendix II.

Personal

1. **What is your job title?** Sales manager

2. **How long have you been working in the company?** I have been working in the company for 7 years and 3 months

3. **Can you explain what cyber security is and why it's important for the company?** Cyber security is the protection of the company's files as well as all the information that is gather both from costumes and the carrier. The reason why it is very import to protect the information is because some of the information is sensitive and could also break the chain of supply. Which has happened to several competitors before. Which could again lead to big delays in the cargo flow all over the world.

General knowledge about cyber security in the company

4. **Do you have any knowledge of cyber security polices within the company? If yes, how did you acquire this knowledge?** Yes, I do. First of all, we have security guidelines for our company. Which handles everything from our cellphone to our personal computer. What you are allowed and not allowed to do on them. We also have courses for cyber security we need to take. As well as this we work as an agent for a carrier, which means we work on their behalf in Norway and they also have a set of rules that we have to ably.

5. **What could be the consequences of an unwanted cyber-attack? And how does this affect your department?** The consequences could be quite large. If a cyber-attack spreads from myself or one of my colleagues to the whole department or even to our principals. The systems are pretty large and there are several thousand people working in the system, so if it spreads to wide everything will stop, and then this would probably cause a disruption with the cargo flow, not only of our company but for companies all over the world. Therefore, it is important to avoid cyber-attacks at any costs.

6. **What do you and your department do to prevent such attacks and have you received any guidelines on how you should work to prevent such attacks?** Yes, we have received guidelines which we are commanded to follow both on our own system and when we are using our principal systems, and they have also set up a lot of trainings that you have to go through. So there are courses and also everyday actions that you need to follow in order to work in the system.

7. **How would you define a proactive security culture? And would you say that the company have been able to create such a culture?** Proactive culture is pretty important, and I think that most big companies now adays have some sort of plan in order to best avoid cyber-attacks. The same goes for our company that has both onboarding and offboarding. We also have a set of rules and guidelines on how you preform your everyday tasks, everything from which programs that needs to be used, that everything needs to be updated and multifactor identification. And also, there is rules on where you can use your software both in Norway and if you're out traveling in terms of not connecting to a public of unsecure WI-FI. There are also rules on where you store all your information and files, so I would say that our IT department makes sure that we have the best possibility to not screw up.

8. **What kind of cyber-attacks do you believe are most threatening to your company and why?** I believe the most common cyber-attacks in towards this industry is Malware, phishing links and some try to scam over the phone, but I don't think it is a big issue in my company at least since we are a small department that collaborate very closely. So, if there is a problem within our company, I think that there might be someone that deliberately tries to hack a server or something and this will be out of our hands.

9. **Do you know about any measures that senior management have implemented to identify and mitigate the potential risks?** We have multifactor identification login system and we also use programs that are pretty resistant regarding phishing and malware such as java script and also personal passwords and one time password that gets send to our phone every morning when we log in, so you need to have a lot of

information to be able to login to someone's user ID. We also use VPN both at home and in the office, and the rules from the IT department are continuously being updated.

Training and awareness

10. **Is cyber security awareness a part of the companies onboarding program?** Yes, it is. When you start the job, you need to go through an onboarding program where you have courses about GDPR to cyber security. You have to read the policies and you also have to use the guidelines in order to use the different programs. And the same for off boarding as well.

11. **Have you had any training about cyber security the last year?** Yes, we have had a course in cyber security from IT department. A 1-hour mandatory course with questionary. And they also send out emails of there are any threats or common issues that they see occur more than once.

12. **How does the company ensure that employees understand and follow security policies and procedures?** Yes, with the guidelines and course. It's a mandatory to read these guidelines and take the courses in order to work in the systems and they are also a part of our daily routine so there is no chance of avoiding the guidelines.

13. **What resources are available to employees who want to learn more about cyber security?** We have an IT department as well as a cyber security manager that handles every request that you send in. At any given point you can ask him if there is anything you would like to know more about or if there is anything that you are suspicious about. Be sights that we have a service desk that helps with everyday problems as well as a lot of anti-virus programs.

14. Considering IMO's recommendation that senior management should lead the development and implementation of cyber security initiatives, do you believe that senior management in your company has taken sufficient steps to improve the training and awareness of cyber security among employees? I think the rules are very strict and there is a reason for that. We have seen the other companies have been hacked and the

consequence of that, so I believe that the employees are forced to follow the new and stricter guidelines that have be implemented by senior management. Everything has become a lot stricter the last couple of years.

15. **Do you believe that the company should prioritize cyber security training and awareness more?** That's a good question. I think in our case when we use it every day we get very used to the rules and you live by them every day and as well with refreshening courses that we get once a year it's pretty hard not to know the rules and guidelines. So, I don't think we need even more cyber security training as long as everything works with our IT department and service desk.

16. **Is there anything else you would like to add to this interview?** No

17. **Could you give me three tips on how to recognize phishing attempt?** That could be a mail from an unknow mail address asking you to press a link or enter a website. You could also get a phone call telling you to give some information in order to solve a problem. Mail of a mail address that is not known to you press a link or a phone.

Personal

1. **What is your job title?** Manager director

2. **How long have you been working in the company?** Eight years

3. **Can you explain what cyber security is and why it’s important for the company?** It's to protect our interest and computer system data. This is important because we need to protect all the software to make sure that we can run the company.

General knowledge about cyber security in the company

4. **Do you have any knowledge of cyber security polices within the company? If yes, how did you acquire this knowledge?** We do frequently get emails and postings on our intranet about updates when it comes to cybersecurity and if there's anything, we need to be aware of, for example a phishing attempt that's going around. There is also mandatory training every year that all the employees need to take.

5. **What could be the consequences of an unwanted cyber-attack? And how does this affect your department?** Well, we could have a complete shutdown for an unknown period. We have seen before that competitors had it for like 3 weeks and there was nothing to do actually. We could close the door and lose a lot of revenue internally.

6. **What do you and your department do to prevent such attacks and have you received any guidelines on how you should work to prevent such attacks?** Yes, not to open any suspicious emails, but of course it's our IT departments that really handles all the security for us so, I think it's quite difficult to come in there. The most important part for us is to be aware of dangers.

7. **How would you define a proactive security culture? And would you say that the company have been able to create such a culture?** Well, always enlighten people of course with what to do and not to do, and there is a lot of

things happening behind the scenes that we have been doing and are doing and certainly there's a refresh renew when new technology comes so we have a lot of setups already that prevented cyber-attacks.

8. **What kind of cyber-attacks do you believe are most threatening to your company and why?** Shut down of computer systems because then we will be blind, and we have no knowledge about our products where the cargo is, and it will be a catastrophe actually. Because there's no papers anymore everything is in the computer system. We might as well close down until we get the computer systems back.

9. **Do you know about any measures that senior management have implemented to identify and mitigate the potential risks?** We have a multi-factor authentication for all our devices, meaning we not only need to import the password, but we also need to input the password together with a code that we get on our cell phone whenever we try to log into the system from an internet outside of the office. I recently got some feedback form or IT department that this multifactor authentication has already prevented quite many attacks.

Training and awareness

10. **Is cyber security awareness a part of the companies onboarding program?** Yes, yes, yes of course they even must sign a contract on what to do and not to do and then they have to confirm that they have read it.

11. **Have you had any training about cyber security the last year?** We have not had any cybersecurity training the last year, but we have gotten some updates by e-mail and on our intranet.

12. **How does the company ensure that employees understand and follow security policies and procedure**s? We must sign a contract with the guidelines, we get some emails and have some training, but we don’t have anything other than that. So I think we could do better more definitely.

13. **What resources are available to employees who want to learn more about cyber security?** It's the IT department in our head office. We can contact and they will help us out if we have any questions or if there's anything that might be suspicious, they will let us know.

14. **Considering IMO's recommendation that senior management should lead the development and implementation of cyber security initiatives, do you believe that senior management in your company has taken sufficient steps to improve the training and awareness of cyber security among employees?** No, I think there's a lot more to do differently. We have done small steps but of course a lot of things happen behind the scenes that we are not aware of.

15. **Do you believe that the company should prioritize cyber security training and awareness more?** No, I don't think so as long as the IT takes measures and make sure we have a multi-factor authentication for all our devices and sends us information if there's anything we need to be and the look on the look on the lookout for out for.

16. **Is there anything else you would like to add to this interview?** No, I don't think so. It's an important task for sure and it will be even more important in the future.

17. **Could you give me three tips on how to recognize phishing attempt?** Firstly, e-mail address is quite easy to spot it also always if you are a doubt click on the properties and check the e-mail address. I mean this is maybe the best thing to do and if you don't know the company don't open e-mail. Otherwise they're quite professional I would say, so make sure you don't open anything unexpected that should not come there and if you're too good to be true it is.

Personal

1. **What is your job title?** Operations export customer services

2. How long have you been working in the company? Four years and four months

3. **Can you explain what cyber security is and why it's important for the company?** Yes, cyber security is to make sure you have the correct program in order to protect and be prepared for cyber attacks. I think it's important for companies to be prepared if there's something, and I think it's more cyber attacks than earlier because everything is more technical now.

General knowledge about cyber security in the company

4. **Do you have any knowledge of cyber security polices within the company? If yes, how did you acquire this knowledge?** I don't actually have a lot of knowledge about it. But I do get some emails from time to time regarding updates and what not to click on when it comes to emails and suspicious links but other than that I don't really have much insight into the cyber security policies in the organization.

5. **What could be the consequences of an unwanted cyber-attack? And how does this affect your department?** I think the consequences of course may be that people that should not have access to information can get that quite easily. If you don't are aware of what to look after when it comes to being hacked. This could lead to consequences that people who should not have access to information get access, this can be customer information and of course private information about the employees. Also, because we do work with a lot of bill of lading and information like that, there is also some private information about our customers that should not be available for everyone.

6. **What do you and your department do to prevent such attacks and have you received any guidelines on how you should work to prevent such attacks?** I don't think my department actually do anything specific or at least that I am aware of, but of

course we have systems that should make it easier for us to do it in a way that we might just do it automatically. Like we have to use the VPN if we are working from home or connection to any other internet outside of the office. I know that there are some guidelines on the intranet, but I'm not really there often, I probably should check in more often.

7. **How would you define a proactive security culture? And would you say that the company have been able to create such a culture?** I think that proactive security culture it's a culture that tries to prevent cyber attacks. I don't really think that we have that just we need to take some courses, but I have been here for 4 years and there's not been that much focus. I know that we did it on the onboarding program, and I know where I can find it on the intranet, but there is no obligated courses to take. I think it should be like once a year or something to go through the information. I know that we have to log in to VPN like I said, and we also get a code on our phone when we try to log in to our system. I know that it is probably more than that, but it is just not very known to the other people in the business that does not work with IT and cyber security.

8. **What kind of cyber-attacks do you believe are most threatening to your company and why?** Exactly, I think maybe to our company would be to get customer information, information about prices and try to blackmail us. I would think that is more threatening than employees personal information of course that is always threatening.

9. **Do you know about any measures that senior management have implemented to identify and mitigate the potential risks?** No actually

Training and awareness

10. **Is cyber security awareness a part of the companies onboarding program?** Yes, there are some courses that we had to take as a part of the onboarding. I think I did that after being at the company for 2-3 weeks.

11. **Have you had any training about cyber security the last year?** No

12. **How does the company ensure that employees understand and follow security policies and procedures?** I have to go back to the e-mail I talked about. We get emails when there are changes in the policies and sometimes, we get emails about threats or just to restart the computer because they need to install some new protection. Other than that, we don’t have anything to confirm that we follow the security policies.

13. What resources are available to employees who want to learn more about cyber security? There is a page on our intranet with the different articles and actually there are a lot of information there. So, it's easily available but I'm not sure what kind of information you would find on the page right now. I haven’t checked it for a long time, but I know that you could find some articles about cyber security.

14. Considering IMO's recommendation that senior management should lead the development and implementation of cyber security initiatives, do you believe that senior management in your company has taken sufficient steps to improve the training and awareness of cyber security among employees? No, I don't know. There might have been something they have done that we are not aware of, but I think a lot of things happen that we don't get information about. I think that senior management should try to be better at communicating what they are doing when it comes to cyber security.

15. **Do you believe that the company should prioritize cyber security training and awareness more?** Yes, I do think so actually. I think it's important these days and you can see other companies in our business that has been hacked, so I think we should talk more about it. And also have some more training about what to look for.

16. **Is there anything else you would like to add to this interview?** No, I don't think so.

17. Could you give me three tips on how to recognize phishing attempt? Oh yes, probably a typical failing space and bad grammar and emails and like very, very long e-mail address its subject or something like that. And if they ask for your credit card details or if they ask for any personal information over Internet that could be a red flag.

Personal

1. **What is your job title?** Part time operations import customer service

2. **How long have you been working in the company?** I've been working in the company for a little over two years

3. **Can you explain what cyber security is and why it's important for the company?** Cybersecurity is how the company secured their data and sensitive information from digital attacks and competitors and that is also why it's important for the company

General knowledge about cyber security in the company

4. **Do you have any knowledge of cyber security polices within the company? If yes, how did you acquire this knowledge?** Very little. I know that my password is my personal key that I can't share with anyone. I also know that I have to stay silent about sensitive data and can share information with others from outside the organization and I mainly got that information through my contract

5. **What could be the consequences of an unwanted cyber-attack? And how does this affect your department?** In an unwanted cyber attack private and sensitive data could be visible for both our competitors and other people that should not have access to that information. Another thing that can happen is that our computer systems shut down and we will not be able to work because we will not have access to the systems that we need.

6. **What do you and your department do to prevent such attacks and have you received any guidelines on how you should work to prevent such attacks?** no i'm not and i don't know any.

7. **How would you define a proactive security culture? And would you say that the company have been able to create such a culture? I** would define proactive security culture on how we as an organization prevent unwanted incidents before they happen. I know that there haven't been any cyber attacks on our company that have caused us and they trouble but I don't feel like I have gotten a lot of information when it comes to cybersecurity.

8. **What kind of cyber-attacks do you believe are most threatening to your company and why?** I know that other competitors have been hacked with a fake e-mail and then they demanded ransom so maybe that's the most threatening thing when it comes to cyber attacks.

9. **Do you know about any measures that senior management have implemented to identify and mitigate the potential risks? I** think so however I haven't gotten any

Training and awareness

10. **Is cyber security awareness a part of the companies onboarding program?** Yes, however I have not gotten any

11. **Have you had any training about cyber security the last year?** No, I have not

12. **How does the company ensure that employees understand and follow security policies and procedures?** It is in our contract when we sign for the company and of course when you start. However, I didn't get the course this is something that I've heard from the colleagues and I don't have any.

13. **What resources are available to employees who want to learn more about cyber security?** I don't know anything except the contract and what we receive in emails from time to time.

14. **Considering IMO's recommendation that senior management should lead the development and implementation of cyber security initiatives, do you believe that senior management in your company has taken sufficient steps to improve the training and awareness of cyber security among employees?** I know that the IT department sends out some emails from time to time, and I guess this on behalf of senior management, but other than that I don't know.

15. **Do you believe that the company should prioritize cyber security training and awareness more?** Yes, I believe so since I haven't got any since I've started two years ago. And I also know that a lot of our competitors have being victims of cybersecurity the breaches that has shut down their whole system, so I think it's very important to have more knowledge about this

16. **Is there anything else you would like to add to this interview?** No

17. **Could you give me three tips on how to recognize phishing attempt?** The first one is if the threats actor is using Gmail and outlook instead of a company name. The second one is if e-mail contains a request on verifying personal information or to transfer money. The third one is if the message contains a lot of grammar errors

Personal

1. **What is your job title?** Operations import customer service

2. **How long have you been working in the company?** 16 years

3. **Can you explain what cyber security is and why it's important for the company?** Cybersecurity is protection from online attacks, but also from simply making mistakes online by releasing sensitive data as well as protecting yourself against attacks from the outside. It's a very big field which I know very little about, but yes that's what initially what hits me when I think about the cyber security

General knowledge about cyber security in the company

4. **Do you have any knowledge of cyber security polices within the company? If yes, how did you acquire this knowledge?** We've had some courses and some mandatory courses, but other than that what we have received from the company it's about using common sense really. It's about remembering what you can do and can't do as well as how to protect yourself from outside attacks you know business. We've been fortunate enough to see how attacks work with other companies not our own and that's kind of been a good wake up call.

5. **What could be the consequences of an unwanted cyber-attack? And how does this affect your department?** Well, an unwanted attack is something that happened to a competitor a few years ago. I remember where their systems went down for several days, that means customers won't get their bookings and customers won't get their arrival notice the system just completely stops. Even if the vessels don't stop and that in turn means there's a backlog when containers arrive you might be able to process them because your systems are simply down. As well as that there are sensitive data that could be stolen you know customer

data and statistics stuff that companies don't necessarily want to share so much of. But the biggest problem would definitely be systems going down for several days. That's the nightmare scenario

6. **What do you and your department do to prevent such attacks and have you received any guidelines on how you should work to prevent such attacks?** We can turn the question around and start with the guidelines first because that's kind of how we work. We do receive from time to time updated guidelines, updated advice and how to how to deal with deal with incoming emails. Our system is well enough so that it removes those very questionable emails, but from time to time these get through and we just simply leak them and if there is it looks like a trusted source, but a questionable link will always check and that is according to the guidelines. If this link is really from the trusted source then we make a phone making call to the customer or the sender and ask if this was really sent for their email. Luckily since we don't deal that much with the IT and security systems. The proper IT protection of the system from Norway it is mostly screening emails and making sure that you do not open those questionable links and we have a good IT department that helps with identifying these for us.

7. **How would you define a proactive security culture? And would you say that the company have been able to create such a culture?** Well see seeing as I say very oddly on that we haven't really had much course except for the mandatory courses that we have to take on new on new systems is introduced or new regulations introduced. I suppose the company could be more proactive, however it's such a small team and the focus that we have on not clicking on links that we don't know where come from, and not opening up attachments we don't know where come from. That is about the extent of what we do also we don't go online and visit questionable sites and stuff like that, even if the system itself doesn't block for it at least the people here at our office do not go around and because it's different questionable sides at work.

8. **What kind of cyber-attacks do you believe are most threatening to your company and why?** I think that questionable links is the most dangerous one because I think the company itself is pretty well protected from outside attacks.

I've described before that's the biggest threat because our system is linked in several countries if someone in another country clicks the wrong link, we risk our system going down completely. Fortunately, there are backup servers and there are backup sites, and everything are constantly backed up so everything can be turned around in 5 minutes. An old assistance can be shut down and new system can be opened up really quickly so that's a backup systems takeover but yes it's outside question on links stuff like that is worried some for us.

9. **Do you know about any measures that senior management have implemented to identify and mitigate the potential risks?** No, not per se I don't know what senior management has thought about this, but from time to time we'll receive emails from IT department pointing out how to identify if there's something questionable going around how to identify that this is wrong and in some or not hints but ideas or suggestions on what to look for but what senior management has done no. Because I believe that it's the IT department that's case

Training and awareness

10. **Is cyber security awareness a part of the companies onboarding program?** Yes, I would say so it's something we talk about from time to time as well so it's in our awareness most of the time.
11. **Have you had any training about cyber security the last year?** No

12. **How does the company ensure that employees understand and follow security policies and procedures?** A mandatory course you have to take online when you started the company, that's it.

13. **What resources are available to employees who want to learn more about cyber security?** There's plenty of resources online on our websites however that's ironic because they've shut that should go down that's gone but yes it's it's mostly online for us we can look it up we can also phone up the you know these IT people and talk to them about if you have questions of course.

14. **Considering IMO's recommendation that senior management should lead the development and implementation of cyber security initiatives, do you believe that senior management in your company has taken sufficient steps to improve the training and awareness of cyber security among employees?** I do believe that was a senior management decision to delegated this to people who know more than them. I think that's the best we can say about senior management contributed because their IT competence might not be that high. We are talking about older people here and of course they have an IT department that's on top of things and follow up on things.

15. **Do you believe that the company should prioritize cyber security training and awareness more?** It's one of those areas I don't think is enough awareness. But criminals become more creative we see it today just opening up the newspaper this morning they get more creative and we have to become more creative in learning about these things. Cyber security it's a field where it's hard to stay ahead you always one step behind because you have to it's not a proactive field it's a reactive field. So, yes I definitely think that focus should be there should be more focused on it, but it's a tough area. I don't think its enough awareness, but you can't go around expecting everyone to be criminals so you need to just pay attention to emails and things that might be suspicious.

16. **Is there anything else you would like to add to this interview?** No not really.

17. **Could you give me three tips on how to recognize phishing attempt?** Well, it is important to check out the e-mail address and if there is a link that they want you to click on you shouldn't unless you know that there's safe to click on the link. I recently read in the newspaper that someone changed the e-mail address with the OS's to be like zero's so it's important to be aware of small things like that.

COMPANY B

Personal

1. **What is your job title?** Sales and marketing manager
2. **How long have you been working in the company?** Five years
3. **Can you explain what cyber security is and why it's important for the company?** To protect the data and information and the systems that we use in our day-to-day job. It's important because it helps us keep are sensitive information private

General knowledge about cyber security in the company

4. **Do you have any knowledge of cyber security polices within the company? If yes, how did you acquire this knowledge?** We get information about the policies within the training program and we also get some emails if there's anything that we need to be aware of.

5. **What could be the consequences of an unwanted cyber-attack? And how does this affect your department?** We could lose sensitive information both our own and our customers. This would lead to a shutdown of the entire system and we wouldn't be able to provide our customers with information about when their cargo will arrive or where their cargo is at this time there will also be a problem when it comes to releasing of the cargo since the systems would be shut down.

6. **What do you and your department do to prevent such attacks and have you received any guidelines on how you should work to prevent such attacks?** In the training courses we get knowledge about how to detect and identify potential phishing and malware attacks. It's a lot of focus on being cautious and

aware of suspicious email or links. Other than that, I don't think I have gotten any guidelines.

7. **How would you define a proactive security culture? And would you say that the company have been able to create such a culture?** I guess awareness and knowledge and I would say that we have a proactive security culture. We pay a lot of attention to the security and we talk about it in the office if there is anything, we need to be aware of.

8. **What kind of cyber-attacks do you believe are most threatening to your company and why?** I think malware and phishing because there's so many parties or people in the company so it's easy to click a link that you're not supposed to click and then gain access to or systems that we use so if they get control of it we are in deep s***.

9. **Do you know about any measures that senior management have implemented to identify and mitigate the potential risks?** I know that they have implemented some measures after we had a cyber attack, but I don't know what.

Training and awareness

10. **Is cyber security awareness a part of the companies onboarding program?** Yes, we have an onboarding program. Once you start you have to complete series of lectures and take a mandatory test.

11. **Have you had any training about cyber security the last year?** Yes

12. **How does the company ensure that employees understand and follow security policies and procedures?** Again, through the online courses which we are mandatory.

13. **What resources are available to employees who want to learn more about cyber security?** Extensive online courses and there's also brochures and articles on the intranet

14. **Considering IMO's recommendation that senior management should lead the development and implementation of cyber security initiatives, do you believe that senior management in your company has taken sufficient steps to improve the training and awareness of cyber security among employees?** Yes, I do think they have done so, but I have faith. But I can't really say for sure.

15. **Do you believe that the company should prioritize cyber security training and awareness more?** Good question, I don't want to be too much and pushy because it can just be annoying.

16. **Is there anything else you would like to add to this interview?** No

17. **Could you give me three tips on how to recognize phishing attempt?** Typos and not spelling things correctly, a weird email address and asking for banking information.

Personal

1. **What is your job title?** Manager director in Norway

2. **How long have you been working in the company?** I have been working with the company for almost 8 years now

3. **Can you explain what cyber security is and why it's important for the company?** Cyber security from my point of view is that the security system that a company has to protect the company and the company information from being attacked works in the right way. That the company's security system protects our data.

General knowledge about cyber security in the company

4. **Do you have any knowledge of cyber security polices within the company? If yes, how did you acquire this knowledge?** Yes, we have the knowledge. We have on a yearly basis a course that we need to take. We also message the employees about current cyber threats and things they need to be aware. and in the same portal where they take the yearly course there are also different articles to read about cybersecurity.

5. **What could be the consequences of an unwanted cyber-attack? And how does this affect your department?** It would harm the company a lot and all the systems would immediately shut down. The Norwegian office as we are purely customer service and sales office right now, this would in theory mean that we will not be able to do anything except using the backup line until we could get back into the system again. The backup is only a very limited part of the system that we're using today.

6. **What do you and your department do to prevent such attacks and have you received any guidelines on how you should work to prevent such attacks?** I mean the major attack coming from the background in the interactive system. We as employees in the company need to be proactive and be aware if there's some suspect e-mail for example coming in to our office. We are more or less told that we should never click a link for example which is coming from a party which seems suspect or we should also always check the e-mail addresses if it's really the real person we have contact with them. In general, we have to be very careful and about how we treat emails and the same goes with protocols, and with someone would call us and ask for a company account number or something like that. We would immediately not give any information but instead hang up trying to ask for the name and the number of the person.

7. **How would you define a proactive security culture? And would you say that the company have been able to create such a culture?** I think the collectiveness is to inform all the users in the company and not only sort of IT or top management and as long as all user are important taking care of this as a daily matter. I think it's a very, very good protection for the company. I hope and think that we are very well prepared and for the decisions in our daily work to protect the company security but again you can never be 100% safe.

8. **What kind of cyber-attacks do you believe are most threatening to your company and why?** I think phishing emails are the most threatening. It might be hard to spot and it can do a lot of damage. We have this phishing alert that you can press as soon as you have a suspect e-mail.

9. **Do you know about any measures that senior management have implemented to identify and mitigate the potential risks?** I think that we as a company are taking security measures all the time. I don't know details about it because it was like very much IT related matters but I'm already following it closely and we are on the high security level the company. I think it's hard for me to give an example on this subject as this one part of my daily job.

Training and awareness

10. **Is cyber security awareness a part of the companies onboarding program?** Yes, it is this academy portal training that's being done by new employees.

11. **Have you had any training about cyber security the last year?** Yes

12. **How does the company ensure that employees understand and follow security policies and procedures?** That's a good question, I think the main driver is to get training that we do and having the IT following that up on a regular basis towards us so if anything would happen. Even if it's a small thing that would be like an internal distribution about this this issue that has occurred and also to follow that up the daily discussions in the in the office would also help yeah to keep the awareness about it.

13. **What resources are available to employees who want to learn more about cyber security?** We have a lot of information on our intranet and IT is always available if you have any questions.

14. **Considering IMO's recommendation that senior management should lead the development and implementation of cyber security initiatives, do you believe that senior management in your company has taken sufficient steps to improve the training and awareness of cyber security among employees?** I would definitely confirm that this has been taking on really high, high level within the company. I mean we even had a cyber attack three years back and after that we saw an extremely higher focus on this issue.

15. **Do you believe that the company should prioritize cyber security training and awareness more?** That's interesting question, I think the attention is really high. I mean I'm sure there always minor achievements that could be done, but honestly personally I'm impressed on how serious this been taken within the company.

16. **Is there anything else you would like to add to this interview?** Yes, I think it's really interesting to be honest these are really interesting and important thing answer. I'm happy to see that you're taking it also from this perspective that you're doing and not just from an IT perspective. Because this is normally where you think it would have importance and research possibilities, but these soft values that how the people in the office that proceeding of the working within the daily macros actually I think more important that we actually expected

17. **Could you give me three tips on how to recognize phishing attempt?** For example, when I get e-mail with the link don't click on the link. Second, I would e-mail address from the company or something that you switch one or two letters in like an e-mail address so the first thing you see I know that person or that e-mail company, but it could be the wrong and then the third one is I would say the signature. It’s almost the same, but there might be some small twitches

Personal

1. **What is your job title?** My job title is import and export customer service

2. **How long have you been working in the company?** I have been working here approximately 10 months

3. **Can you explain what cyber security is and why it's important for the company?** Cyber security is protection of information in our data system and it's important to not be hacked or not to get stolen from. Criminals can use this information for another purpose.

General knowledge about cyber security in the company

4. **Do you have any knowledge of cyber security polices within the company? If yes, how did you acquire this knowledge? I**'m not 100% sure so I'm going to answer no.

5. **What could be the consequences of an unwanted cyber-attack? And how does this affect your department?** If there would be a cyber attack it will be a crisis. We could lose all the personal details for from our customer and blocking off us for working as normal, and the consequences will be total shut down until the problem is solved.

6. **What do you and your department do to prevent such attacks and have you received any guidelines on how you should work to prevent such attacks?** We have an Academy where we have to go through with courses about cyber security or learning about or get informed about the cybersecurity. I know about that and our head office will send some fake mails and just to trick us or test us if we're going to answer them or report them as a catfish or what we call it.

7. **How would you define a proactive security culture? And would you say that the company have been able to create such a culture?** Both yes and no. We have quite strict rules and procedures when it comes to log-in in our system outside of our office if that can be counted as proactive.

8. **What kind of cyber-attacks do you believe are most threatening to your company and why?** I will think phishing emails could be the most threatening because we're getting quite a lot of those and it's some phishing emails looks like legit, but if you dig a little bit deeper and see where the mail is coming from you can obviously it's see that it's catfish or hacker or something. Other than that, from our side from the customer service side I am not sure because we have a quite good system to block unwanted websites but it's not all the catching everything from the emails so I think that is the biggest let's

9. **Do you know about any measures that senior management have implemented to identify and mitigate the potential risks?** No, i'm not sure so pass

Training and awareness

10. **Is cyber security awareness a part of the companies onboarding program?** If you mean the training program. I know that we have to look through some guidelines or videos on the Academy that we're having and otherwise they're reporting the maze that head office is testing us on other than that I am not sure I have not been apart of any other than the Academy or the test I know that our IT department is working in the background if something is happening but I don't know

11. **Have you had any training about cyber security the last year?** yes through the Academy training

12. **How does the company ensure that employees understand and follow security policies and procedures?** I think the first is what I mentioned earlier that

the head office is going to test us sometimes on the mail, but other than that it's based on trust.

13. **What resources are available to employees who want to learn more about cyber security? I** can of course contact the IT department and they will got you through a lot of materials if you want to learn more you can always it's a lot of you have videos or you can take it in the Academy, but other than that I don’t know.

14. **Considering IMO's recommendation that senior management should lead the development and implementation of cyber security initiatives, do you believe that senior management in your company has taken sufficient steps to improve the training and awareness of cyber security among employees?** Of course, I think they are sure about it and they always mention it when we start working but it could always be improved, I like this into you I recognize how but I'm not so educated regarding the cyber security so of course we can improve it's always included

15. **Do you believe that the company should prioritize cyber security training and awareness more?** Yes of course because we are uh focusing a lot of towards customer and sending out a lot of main nuts internally but externally so the risk is maybe a little bit bigger to get something that you don't want so of course we should have more education or tests or anything.

16. **Is there anything else you would like to add to this interview?** No

17. **Could you give me three tips on how to recognize phishing attempt?** Three examples to recognize the first one is obviously the main address that's coming from and the second maybe looking for contents in the mail that's where you see the third and wanted application on your on your computer if you get something that's you didn't unfold or something like that

Personal

1. **What is your job title?** Customer service officer export

2. **How long have you been working in the company?** For two months

3. **Can you explain what cyber security is and why it's important for the company?** Cybersecurity is to protect the company's files and information. This is important in order to avoid cyber attacks such as ransom and phishing attempts

General knowledge about cyber security in the company

4. **Do you have any knowledge of cyber security polices within the company? If yes, how did you acquire this knowledge?** I have got some emails about cybersecurity and I have also had some training when I started this job. I also know that we have to use a two-step identifier to be able to access our systems other than that I don't really have any knowledge about the policies.

5. **What could be the consequences of an unwanted cyber-attack? And how does this affect your department?** System and programs, we are working in could shut down. This could lead to economic consequences and closing the office for a period of time. For my department we are not able to and give customers all the information they need if you don't have access to the programs and systems that we're working in.

6. **What do you and your department do to prevent such attacks and have you received any guidelines on how you should work to prevent such attacks?** Yes, and as I said we have the two-step identifier to login to the system. I have just started in the company, so I had some computer-based trainings about how to not open emails that look suspicious and attachment that's in our emails.

7. **How would you define a proactive security culture? And would you say that the company have been able to create such a culture?** I think you just have

to be aware of things that pops up on your computer as well as suspicions emails. I was told by my colleagues that our company had cyber-attack a couple of years ago, and after that everything changed. It became a lot stricter when it comes to not clicking links and things like that.

8. **What kind of cyber-attacks do you believe are most threatening to your company and why?** And the previous attack was a ransom attack, so I think that is the most threatening.

9. **Do you know about any measures that senior management have implemented to identify and mitigate the potential risks?** Yes, I think they have. I'm not sure, but since they have started all this two steps authentications programs, I think that's one new thing they're doing we're trying to implement.

Training and awareness

10. **Is cyber security awareness a part of the companies onboarding program?** Yes, I just had it

11. **Have you had any training about cyber security the last year?** Yes

12. **How does the company ensure that employees understand and follow security policies and procedures?** First we have we have to implement all the two steps authentications and programs that we need to for instance working from home. We also have a mandatory test when we do the cyber security training and you need to pass this test.

13. **What resources are available to employees who want to learn more about cyber security?** We have this Academy website where we have all the courses and trainings.

14. **Considering IMO's recommendation that senior management should lead the development and implementation of cyber security initiatives, do you believe that senior management in your company has taken sufficient steps to**

improve the training and awareness of cyber security among employees? I don't know anything more than the implementation of the two step identifier.

15. **Do you believe that the company should prioritize cyber security training and awareness more?** I think that it depends on which country you are working in and I think in Norway we have all the necessary training and are well aware.

16. **Is there anything else you would like to add to this interview?** No

17. **Could you give me three tips on how to recognize phishing attempt? It can be a** suspicious email if it's not well written in Norwegian or English for instance, you should be aware and not open the attachments or links in emails or in SMS.

Personal

1. **What is your job title?** Customer service export

2. **How long have you been working in the company?** Approximately 2 years

3. **Can you explain what cyber security is and why it's important for the company?** It's to prevent any attacks on the company and it's important in order to safeguard all of your documents and all of your sensitive information

General knowledge about cyber security in the company

4. **Do you have any knowledge of cyber security polices within the company? If yes, how did you acquire this knowledge?** We do have regular sessions training sessions which is sent out on a yearly basis from head office which we have to mandatory complete within like a certain time frame

5. **What could be the consequences of an unwanted cyber-attack? And how does this affect your department?** We could get sensitive information going around and this could result in losing customers, losing business and a lot of financial loss.

6. **What do you and your department do to prevent such attacks and have you received any guidelines on how you should work to prevent such attacks?** We have the two-phase authentication, so we have to either use an app or like a login password. We also have something called set scaler which you have to log into before you're able to connect to say a Wi-Fi that isn't your computer or your Wi-Fi at work.

7. **How would you define a proactive security culture? And would you say that the company have been able to create such a culture?** I would say that ensuring that everybody takes use of the two-factor authentication and actively makes sure that they don't click on phishing mails and anything like that, and I would say that our company is quite forward in doing so.

8. **What kind of cyber-attacks do you believe are most threatening to your company and why?** I'd say maybe phishing emails is most threatening because some of them are quite sophisticated so it can be quite hard to see that it's from a phishing malware sort of thing and I think that would be the most threatening because it's quite easy to just click on a link or downloading a Word document which would then infect your computer.

9. **Do you know about any measures that senior management have implemented to identify and mitigate the potential risks?** I would think that would be the training modules as well as the authentication measurements

Training and awareness

10. **Is cyber security awareness a part of the companies onboarding program?** Every new employee has to go through the mandatory training and every year you have to it

11. **Have you had any training about cyber security the last year?** Yes

12. **How does the company ensure that employees understand and follow security policies and procedures?** The things that could be through examples we did have a cyber security attack two years ago and we saw the effects of that, and this is also shown in the training modules showing like if you are subject to an attack these are the outcomes

13. **What resources are available to employees who want to learn more about cyber security?** That would mainly be the training module and I do believe there's a team at that office which you can send an e-mail to just to ask them if there's anything you're uncertain about.

14. **Considering IMO's recommendation that senior management should lead the development and implementation of cyber security initiatives, do you believe that senior management in your company has taken sufficient steps to improve the training and awareness of cyber security among employees?** I

would say that for as long as I've worked there it's been quite sufficient apparently it wasn't before considering that there was an attack, but they really implemented a lot of good measurements in the wake of that.

15. **Do you believe that the company should prioritize cyber security training and awareness more?** At the moment I believe it's sufficient, but it does take quite a lot of time out of your everyday work so if you were to say do it once a month that would be too much, but like a yearly refresher maybe like 1/2-year refresher I think that should be enough.

16. **Is there anything else you would like to add to this interview?** No

17. **Could you give me three tips on how to recognize phishing attempt?** Check the e-mail sender, check for spelling mistakes, and if they're asking for anything sensitive information