Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Economics and Management
Dept. of Industrial Economics and Technology Management

Embla Jenssen
Sindre Johansen

Alignment of cyber risk management in the maritime domain

A case study of a Norwegian maritime technology provider

Master's thesis in Industrial Innovation and Digital Security
Supervisor: Eirik Bådsvik Hamre Korsen
June 2023

NTNU
Norwegian University of Science and Technology

Embla Jenssen
Sindre Johansen

Alignment of cyber risk management in the maritime domain

A case study of a Norwegian maritime technology provider

Master's thesis in Industrial Innovation and Digital Security
Supervisor: Eirik Bådsvik Hamre Korsen
June 2023

Norwegian University of Science and Technology
Faculty of Economics and Management
Dept. of Industrial Economics and Technology Management

NTNU
Norwegian University of
Science and Technology

Abstract

The maritime industry is rapidly transitioning to digitalization and autonomation. New technologies, new environmental regulations, increasing transport volumes and shortage of workforce is driving the development. With digital development comes an increasing need for better cybersecurity and cyber risk management. The purpose of this thesis is therefore to gain insight into cybersecurity in the maritime domain with an emphasis on alignment of risk management efforts. Our research question is therefore:

> *What are the most important building blocks for achieving alignment between middle managers and cyber professionals?*

To answer this question, we chose a single case study research design. The case-organization is a large, maritime technology organization. We have performed in-depth interviews with five middle managers and three cyber professionals. These interviews were analyzed through a within-case and cross-case analysis. The goal of the interviews was to identify potential alignments and misalignments between the two groups.

We found that the responsibility of cybersecurity and technological control is mainly viewed as a siloed part of the IT department. From middle managers' view, cyber risk management is technological controls and compliance, while from the cyber professionals' view, there is a need for internalization of cybersecurity behaviors. To leverage this alignment, we found organizational culture and shared domain knowledge to be the most important building block. These will in turn influence behavior, awareness and communication. Together, these will improve alignment between middle managers and cyber professionals. In addition, middle managers are important intermediaries, as they can bridge the gap between cyber professionals and the organization.

Sammendrag

Den maritime industrien utvikler seg raskt mot digitalisering og autonomi. Utviklingen drives av nye teknologier, nye miljøkrav, økende transportmengder og mangel på arbeidskraft. Med digital utvikling øker behovet for bedre cybersikkerhet- og risikostyring. Målet med denne masteroppgaven er å få innsikt i cybersikkerhet i det maritime domene, med et spesielt fokus på alignment av risikostyring. Forskningsspørsmålet er derfor:

> *Hva er de viktigste byggestenene for å oppnå alignment mellom mellomledere og cyberansatte?*

Vi har valgt en singel casestudie som forskningsdesign for å besvare forskningsspørsmålet. Case-organisasjonen er en stor, maritim teknologiorganisasjon. Vi har utført dybdeintervjuer med fem mellomledere og tre ansatte innen cybersikkerhet. Disse intervjuene ble analysert gjennom en «within case» og «cross-case»-strategi. Målet med intervjuene var å identifisere mulige alignments eller misalignments mellom de to gruppene.

Vi fant at ansvaret for cybersikkerhet og teknologiske kontrolltiltak i hovedsak er sett på som en silo tilhørende IT-avdelingen. Fra mellomledernes perspektiv er cyber-risikostyring teknologiske kontrolltiltak og overholdelse av retningslinjer, mens fra cyberansattes perspektiv er det et behov for å internalisere cybersikkerhetsatferd. Videre fant vi at organisasjonskultur og delt domenekunnskap er viktige byggestener for alignment. Disse påvirker igjen atferd, awareness og kommunikasjon. Sammen vil disse forbedre alignment mellom mellomledere og cyberprofesjonelle. I tillegg er mellomledere viktige mellomledd, da de kan bygge bro mellom cyberprofesjonelle og resten av organisasjonen.

Preface

This master thesis is the final work of our master's degree in Industrial Innovation and Digital Security at the Norwegian University of Science and Technology in Gjøvik, Department of Industrial Economics and Technology Management. The thesis was written during the spring of 2023.

In this research project, we have interviewed actors from a large maritime organization. To all the interview objects; We are very grateful for your time and engagement – your experiences have been highly valuable for the work of this thesis.

With no prior knowledge of the maritime industry, we have dived into a domain which was completely new to us. During the project, we had a series of unexpected events and struggles, and researching within an unknown field has both been exciting and challenging, which is all the more reason to be proud of the finished product. We would therefore like to first thank each other for the collaboration and commitment to this project. Through this work we have complemented each other´s strengths and weaknesses, been constructive in giving and receiving feedback and criticism, and all in all learned a lot from each other.

We would like to show our appreciation to our supervisor, Eirik Bådsvik Hamre Korsen, the study program leader, Halvor Holtskog, and the student advisor, Monika Valset.

Thank you, Eirik, for being of much help and support. Especially during the late stages of this project. Eirik has helped us move forward at difficult times and provided valuable feedback along the way.

Thank you Halvor and Monika, you have greatly contributed to the quality of the study program and our satisfaction as students at NTNU. Halvor has also been present and assisted us when needed during the work of our master's thesis, and Monika has been a big support for all the students at Industrial Innovation and Digital Security.

Finally, we want to thank family, friends, and significant others for their support during these two years, and everyone else who has contributed to this thesis. Many people have been involved in this work who all deserve our gratitude for their contribution.

Gjøvik, June the 9th 2023

Embla Jenssen and Sindre Johansen

List of Figures

List of Tables

1 Introduction

Cyber risks for organizations continue to cumulate, despite increased spending and focus on cybersecurity (Eling et al., 2021). According to the Norwegian National Security Authority (NSM), threats have developed from attacks on little secure home office solutions and phising, to compromising infrastructure and political revenge actions (NSM, 2022). Cyberwarfare is becoming more common, and the ongoing war in Ukraine has implied a paradigm shift in Europe. Activities related to "information warfare" are performed by state actors, where such warfare is an ongoing activity regardless of the relationship of the opponent. Particularly vulnerable sectors are technology corporations, research and development, and public administrative bodies (NSM, 2022). NSM (2022) call for Norwegian businesses to be prepared and reduce their own vulnerabilities. Weak links can cause big consequences, and businesses have to meet cyber risks of tomorrow.

Cyber risks differ from typical business risks (Marotta & McShane, 2018). First, perpetrators are almost always one step ahead because they adapt to defense mechanisms almost faster than they are implemented. Second, a single cyber-attack can harm multiple parts of the organization at once, with less required effort than any other physical attack. However, the IT department, where cybersecurity often is embedded, are separated from the rest of the organization (Manfreda & Štemberger, 2019; Ward & Peppard, 1996). This gap between IT and business has resulted in multiple studies on business-IT *alignment* (Luftman et al., 2017). Furthermore, silo-based approaches can also be found in risk management, where mitigations and measures of risks are applied independently (Hopkin, 2018). While most organizations operate in some form of silos and view them as necessary, they can also create barriers and fragmentation (de Waal et al., 2019). Althonayan and Andronache (2019) argue that cybersecurity management is a multi-faceted strategy that ingrain risk controls and oversights at all levels of the organization.

Multiple authors call for cyber risk managers to shift their focus from technological challenges to social challenges (Li et al., 2019; Soomro et al., 2016; Østby et al., 2020). Despite extensive use of frameworks such as the ISO/IEC 27000-series, organizations continue to struggle with implementing effective cybersecurity (Kosub, 2015). The effectiveness of these standards depend on employee's compliance to policies (Safa et al., 2016). Studies such as Hu et al. (2012) emphasize the role of top management in compliance, but immediate supervisors such as middle managers have more effect on employee attitudes (Liu et al., 2011). Cybersecurity can no longer be a silo in the IT department, and managers need to work together with IT specialists to manage cyber risks in a holistic manner (Marotta & McShane, 2018).

The need for better cyber risk management is evident. We have therefore chosen to scrutinize the relationship between two strategic actors in alignment of cyber risk management and answer the research question:

> *What are the most important building blocks for achieving alignment between middle managers and cyber professionals?*

To answer this question, we selected a qualitative approach. The research design can be described as a single case study with embedded units (Yin, 2018). In this design, one looks at subunits within a larger case and collects data from these subunits. This data is then

analyzed through within-case and cross-case analysis, adapted from Ayres et al. (2003). The data was gathered through interviews with both cyber professionals and middle managers from a maritime technology provider.

Our main findings are that alignment requires a shared purpose, which can be achieved through organizational cybersecurity culture and shared domain knowledge between cyber professionals and middle managers.

1.1 Cybersecurity in an industry built on legacy systems

As one of the oldest industries, the maritime industry has become an indispensable instrument for global trade. The industry is now experiencing a digital transformation due to new digital technologies, new environmental regulations, increasing transport volumes and shortage of workforce (Cicek et al., 2019; Kilpi et al., 2021). At the same time, the maritime industry is facing cyber threats from organized criminal actors (Department of transport UK, 2017). Lack of processes in place for upgrades of legacy systems, inadequately trained staff and untested or missing contingency plans are some of the vulnerabilities that put maritime actors at risk (BIMCO, 2021; DMA, n.d.).

Despite evidence of cyber-attacks from 2010 and onwards, it is less than a decade ago since the maritime industry and academia began giving cybersecurity appropriate attention (Bolbot et al., 2022; Hopcraft & Martin, 2018; Meland et al., 2021). The European Network and Information Security Agency (ENISA) stated in a report from 2011 that cybersecurity awareness in the maritime sector at the time was "very low level or even non-existent" (ENISA, 2011). The same report also found that the regulations in the sector did not provide adequate considerations for cybersecurity. However, the industry regulations and requirements are changing. For instance, the International Association of Classification Societies (IACS) has published new Unified Requirements for cybersecurity, which will become mandatory from 1 January 2024 (IACS, n.d.). The requirements include identification and protection against cyber threats, security capabilities of components and systems, response- and recovery, incident detection and scope of applicability. Det Norske Veritas (2022) further recommends especially product suppliers to implement cybersecurity into relevant management systems, ship design and control systems.

1.2 Definitions and terminology

1.2.1 Cybersecurity and risks

We have chosen to use the term cybersecurity in this thesis. Cybersecurity as a concept is wider than the concept of information security (Von Solms & Van Niekerk, 2013). Information security is essentially protection of information. While cybersecurity also encompasses the protection of assets that can be reached via cyberspace and those that function in cyberspace. Based on the scope of the definition of cybersecurity, cybersecurity risks are furthermore defined as potential harm to individuals or assets, and thus organizational operations. To avoid long-drawn-out terms such as cybersecurity risk management, we will for the most part shorten cybersecurity risks to cyber risks.

We have chosen to include some literatures using the term "information security". Despite the narrower scope, we believe that the underlying logic and arguments are still relevant for the thesis. In cited literature where "information security" is used, we will consider the applicability.

1.2.2 Management terminology

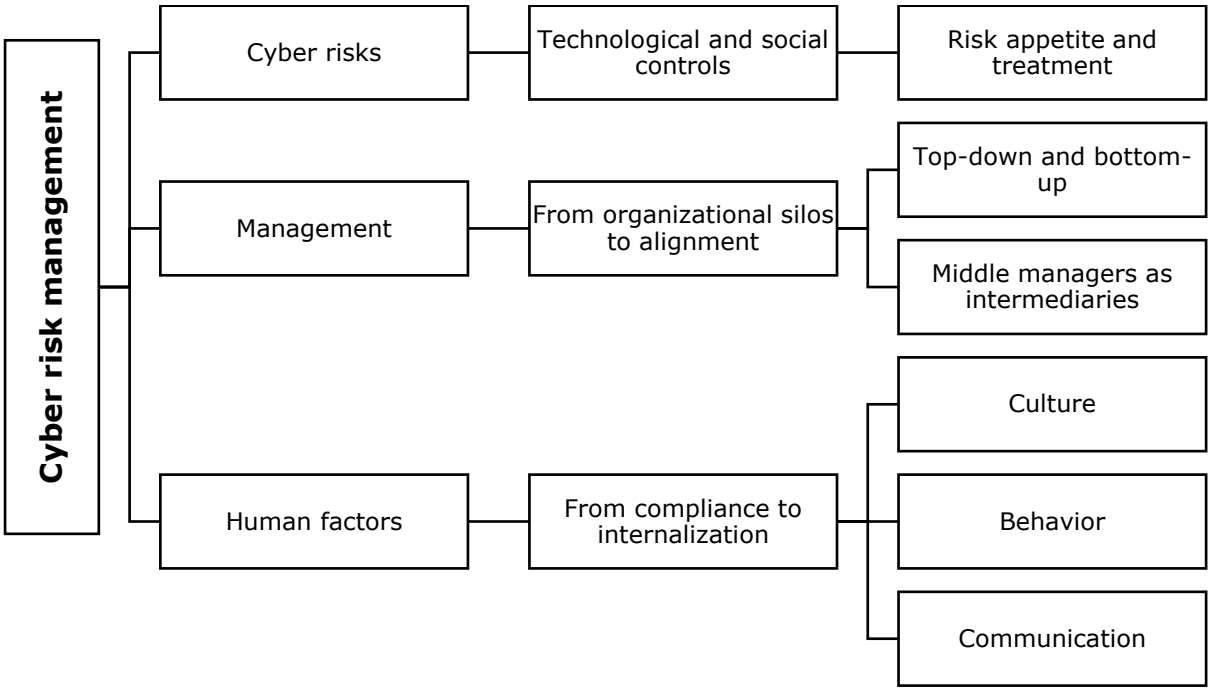
The term *middle manager* does not have a unanimous definition (Rezvani, 2017). Most authors agree that a middle manager is someone who is between top level and lower level. However, there is a range of different descriptions of tasks and role. We have chosen a description by Broussine and Guerrier (1983). They describe a middle manager as someone who is a communicator and coordinator, rarely have the authority to formulate policy and are answerable for implementing policy. We believe this description is the most adjacent to our interview objects.

The definition of a *cyber professional* is loosely based on the description of a certified information systems security professionals in Furnell et al. (2017). However, this description is aimed at security consultants, network architects, chief information security officers and security analysts, and encompass formal requirements. Therefore, we define cyber professionals as someone who works specifically with cybersecurity and has extensive knowledge within the field. As with cybersecurity risk, we will shorten this term to cyber professionals.

2 The literature's perspective on the interplay between cybersecurity, management, and human factors

To provide a structured presentation of the theoretical background, we have created a logic tree of theoretical themes. With cyber risk management as a point of departure, we will explore cyber risks, management, and human factors. These main themes will branch out into several subthemes, as shown in Figure 1.

Figure 1: Logic tree of theoretical themes



2.1 Cyber risk management

Integrated cyber risk management is becoming vital to tackle increasingly sophisticated cyber-attacks and their severe consequences (Khan et al., 2011; Kosub, 2015). Most organizations have a cyber risk management function that covers risk and compliance within information and computer security (Drew, 2007). One of the most commonly used standards for information security management is the ISO/IEC 27001, from now on referred to as ISO 27001 (Kosub, 2015). This standard provides guidance on information security management systems (ISMS), which is based on the plan-do-check-act (PDCA) cycle. Top management lays the foundation of the system through determining risk appetite and treatment strategies (*plan*). The lower levels are given certain guidelines for their work (*do*), and then the top-level review the progress (*check*). Shortcomings and failed objectives are then to be improved (*act*) (Kosub, 2015; Watkins, 2013). The PDCA-cycle is a general tool for quality management but should also be applied to cyber risk management. The key idea is that the PDCA-cycle will lead to continuous execution and improvement of risk management.

Based on ISO/IEC 27001, Kosub (2015, p. 621) present an operational approach to risk management. This approach includes risk identification, risk assessment and evaluation, risk response and risk control objectives, and risk governance and risk culture:

1. *Risk identification*: Define and understand firm's business model, business objectives and assets; determine relevance of IT for business; agree on level of IT security.
2. *Risk assessment and valuation*: Quantify risk (qualitatively or quantitatively) by determining probability of occurrence and estimated impact of cyber risk event.
3. *Risk response:* Decide adequate solutions for risk avoidance, risk mitigation, risk transfer and risk acceptance.
4. *Risk control objectives:* Monitor and proactively control risks and regularly check adequacy of risk response measures.
5. *Risk culture and risk governance:* Focus on company-wide risk culture and create risk awareness among all employees; and provide regular trainings and instructions on IT security for all employees.

2.2 Cyber risks

Eling and Schnell (2016) classifies cyber risk according to the activity, type of attack and source. Cyber activities are either criminal or non-criminal, while type of attack can be attacks such as malware, spam, insider attacks or denial of service (DoS). The source of cyber risks can stem from criminals, terrorists and governments, but also low-level criminals such as script-kiddies (Eling et al., 2021; Whitman & Mattord, 2019).

Cyber risks are fundamentally different from other types of risks. First, Eling and Schnell (2016) described "cyber" as consisting of two constitutive elements: electronic communications (networks) and virtual reality. The first element, networks, describes every network that connects to IT systems. The latter element, virtual reality, "emphasizes the intangible nature and therefore the difficulties in assessing the losses" (Eling & Schnell, 2016, p. 476). Second, cyber criminals have an asymmetric information advantage and only have to find and exploit one vulnerability (Marotta & McShane, 2018). Defenders, on the other hand, must defend and protect every vulnerability. Third, Marotta and McShane (2018) further state that as one criminal can attack multiple organizations at once, the organization's security is dependent on the security of other entities such as suppliers and contractors.

2.2.1 Technological and social controls

Many industry experts and academia still view technological control as the primary solution for cyber threats (Alshaikh & Adamson, 2021). Organizations have become, to an extent, overly dependent on information technology tools for conducting their business (Singh et al., 2013). As only 26% of cybersecurity problems can be solved by technological controls (Cisco, 2018), such controls alone are insufficient in meeting cybersecurity challenges and risks.

Human factors are increasingly being exploited in a variety of attack scenarios due to increased sophistication of attacks (Khan et al., 2011). Most cyber-attacks nowadays include some form of social engineering. That is – psychological manipulation through impersonating an important client or similar, to make the target perform specific actions or reveal specific information (ENISA, n.d.). This makes humans one of the weakest links

in cybersecurity. Therefore, organizations must shift their focus from technological challenges to social challenges (Li et al., 2019; Soomro et al., 2016; Østby et al., 2020).

2.2.2 Risk appetite and treatment

An essential part of risk management is to define a risk acceptance level, also referred to as risk appetite (Kure et al., 2018). The risk appetite is typically defined by the top management, and should be followed at all levels of an organization. The risk appetite level that is agreed upon depends on the type of organization, threat environment, criticality of systems and operations, and the potential consequences in case of an incident (Whitman & Mattord, 2019). Small and medium-sized enterprises (SMEs) will usually have different risk appetites than large corporations that are in possession of larger amounts of wealth and sensitive information. Smaller organizations usually have milder threat environments as they are less likely to be targeted by malicious actors. Therefore, it is important to define an appropriate risk appetite level for each individual organization (Whitman & Mattord, 2019).

How a business decides to treat their identified risks depend on their risk appetite and treatment strategies. Whitman and Mattord (2019) distinguish between five different risk treatment strategies:

- *Defend* – applying measures to reduce or remove the uncontrolled risk.
- *Transfer* – transferring the risk to a different place or another actor.
- *Mitigate* – reducing the impact of an incident in the case of vulnerabilities being exploited.
- *Accept* – choosing to accept a risk as it is, after a formal evaluation.
- *Terminate* – terminating the asset or activity associated with the risk.

Consistent risk management processes require clear guidelines within the organization. Risk treatment strategies are often connected to other strategies, such as different activities in the organization. For instance, an organization can decide to accept residual risk outside of the risk acceptance level because further treatment is undesirable, for example constraining an important business activity. If an organization wants to accept risk which is outside the defined risk acceptance level, it should be based on a conscious business decision and approved by the management (Whitman & Mattord, 2019).

2.3 From organizational silos to alignment

Despite standards such as ISO 27001, organizations continue to struggle to implement successful cyber risk management (Drew, 2007; Kosub, 2015). Marotta and McShane (2018, p. 435) argue that "organizations can no longer afford to let cybersecurity dwell in a technical silo". Cyber risks should therefore be handled by a cross-functional risk management approach. Jarjoui and Murimi (2021) further argue that business-IT alignment is a crucial factor in the coordination of organizations' efforts to combat cyber risks.

Most organizations operate in some form of silos (de Waal et al., 2019). Silos can be beneficial for effective operation when managing a large number of people within an organization, and in allocation of responsibilities and accountabilities within a hierarchy. However, silos can also lead to "silo mentality", where groups, teams or departments do not want to act as "one business" and share knowledge, skills or information. Such mentality is likely to cause less innovation and performance, as well as lower customer outcomes. Furthermore, it can hinder cross-boundary collaboration and cooperation, which is necessary to tackle cyber risks (Jarjoui & Murimi, 2021; Marotta & McShane, 2018).

As silos cause closed departments and groups, it is a natural assumption that silos also cause misalignments of processes, activities and goals. According to Kathuria et al. (2007), alignment requires a shared understanding of objectives and goals both by managers at various levels, but also within various units of the organizational hierarchy. Organizational alignment can further be vertical or horizontal. Vertical alignment refers to the configuration of objectives, decisions, action plans and strategies at different levels of the hierarchy. Horizontal alignment is primarily relevant to the lower levels of the hierarchy and refers to coordination of efforts across the organization. This requires cooperation and exchange between various functional activities.

Alignment research has been performed in several different literatures, including the information systems (IT) literature (Kathuria et al., 2007; Luftman et al., 2017). Such alignment is referred to as business-IT alignment. Business-IT alignment can on one hand be horizontal across the organization, or vertical between IT and top management. The Strategic Alignment Model (SAM) is one of the most commonly used models to study business-IT alignment (Aversano et al., 2012). Through the SAM-model, Luftman et al. (2017) find the following constructs to have a significant impact on alignment:

1. *Communications*: refers to the quality and intensity of the interchange of information, knowledge and ideas between IT and business. Communication results in trusted relationships and increased mutual understanding.
2. *Value analytics*: IT continues to face challenges in demonstrating its value to the business. Value analytics therefore refers to the use of metrics to demonstrate IT contributions in a way that business understands.
3. *IT governance*: refers to allocation of authority and processes for IT, and the business' priorities and allocation of resources. Boundary management of the IT function and resource allocation processes are some of the key activities. In addition, the focus of governance should be activities that create a shared direction.
4. *Partnering*: Refers to the relationship between IT and business. This includes degree of trust, definition of roles and perceived contribution. This can be easier to achieve with cross-functional teams that help to understand shared strategies.
5. *Dynamic IT scope*: refers to IT capabilities and the broader impact of IT services. A dynamic scope is about generating shared activities that foster a flexible IT infrastructure, applying emerging technologies and evaluation.
6. *Business and IT skills development*: refers to human resources practices and activities, such as training, performance feedback, hiring, individual skill development and career opportunities.

The dynamic IT scope-construct will not be discussed further. This is because it mainly refers to technical IT capabilities, which is out of scope for this thesis.

Despite cybersecurity becoming an increasingly important part of business, it is evident that cybersecurity is facing the same challenges as IT did fifty years ago. Manfreda and Štemberger (2019) describe the IT department as going from a closed and ignored unit by the management in the 1970s, to be an important part of the growth of technology and systems for general business use. Nonetheless, many organizations still struggle to close the gap between business and IT (Alaceva & Rusu, 2015).

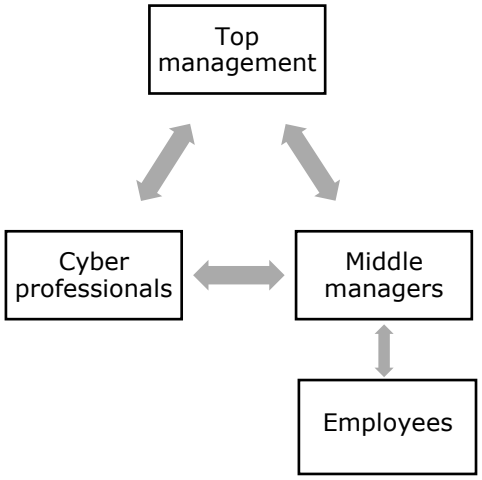
Manfreda and Štemberger (2019) measure the maturity of the relationship between business and IT through a partnership construct. This construct is based on the

abovementioned partnering construct from Luftman et al. (2017). They find that the most influential factors on the business-IT relationship are: respect of the top management, trust, long-term cooperation, open and honest communication, mutual reliance, and commitment to a good relationship. Manfreda and Štemberger (2019) further indicate that knowledge on both the IT and the business side is important.

While the finding suggests that better business-IT alignment is at the hands of both parties, the knowledge of IT personnel is especially emphasized. According to Manfreda and Štemberger (2019), a high level of business and managerial knowledge, resulting in business-oriented IT personnel, had a positive influence on the relationship. High level of technical knowledge and thus technology-oriented IT personnel on the other hand, had a negative effect. They argue that technical-oriented IT personnel is important, but departments neglecting the business role is creating the gap between IT and business. Similar discoveries can be found in Preston and Karahanna (2009). They suggest that chief information officers should articulate issues in business terms and avoid technical jargon. They should furthermore focus on shaping and managing the expectations of top management regarding information systems´ capabilities.

With general and business-IT alignment theories established, we would like to direct the attention towards alignment between top management, cyber professionals and middle managers. As mentioned, business-IT alignment can be viewed as both vertical and horizontal alignment. Vertically, there is a relationship between cyber professionals (IT) and top management (business). Horizontally, there is a relationship between cyber professionals (IT) and middle managers (business). At the same time, as demonstrated in Figure 2, top management, cyber professionals, and middle managers are interdependent on each other. Middle managers are an important intermediary because they implement initiatives from both top management and cybersecurity initiatives downwards to their employees. They are also an important factor for bottom-up initiatives. Vertical alignment from a risk management perspective and middle managers as intermediaries will be further discussed below.

Figure 2: Interdependencies between top management, cyber professionals, and middle managers



2.3.1 An integrated top-down and bottom-up approach to risk management

Kathuria et al. (2007) describe vertical alignment as when there are consistencies between strategic management and strategic implementation. Strategic management are strategies developed at the top level of the organization and is iterated down, while strategic implementation is carried out at the bottom level. Such approaches are also common in risk management and are described as top-down and bottom-up approaches (Linkov et al., 2014). Both the top-down and the bottom-up approaches can be found at the same time in many organizations – for example in different departments or projects within the organization. They can also coexist and overlap, for example in the form of top-down planning and bottom-up learning processes.

The top-down approach is built on the idea that managers and other decision-makers should lay the foundation for successful efforts in an organization (Linkov et al., 2014). Here, one begins with assessing the responsibilities of top management and understanding how one can incorporate goals, strategies, and value to the rest of the organization. It is the manager´s job to facilitate good conditions for performance downwards in the top-down approach (Linkov et al., 2014). In contrast, the bottom-up approach begins at the lower end of the organization and moves incentives and ideas upwards. Which methodology is best suited depends on the organizational context, and under many circumstances the top-down approach is disputed. According to Tessier and Otley (2012), the top-down approach can easily lead to a command-and-control environment within the organization if not carefully managed.

The bottom-up approach on one hand may be better suited in situations where the employee´s opinions, decisions and innovative freedom should be emphasized. On the other hand, Tessier and Otley (2012) also highlight that where there is need for standardization and consistency of work routines and procedures, a well-managed top-down approach can be beneficial. Well-managed hereby means that the foundation and standards are set by the top level of the organization, but without becoming overly controlling towards the employees. The desired outcome is to achieve high performance within certain boundaries. The organization should work under certain guidelines to ensure the required consistency, while at the same time maintaining an empowerment-oriented environment as opposed to a controlling environment. From a cybersecurity and risk management perspective, top-down would cover the facilitation and formalities, for example incorporating risk management frameworks. The bottom-up aspect would on the other hand build engagement, incentives and learning from the lower levels and move these upwards in the organizational hierarchy.

2.3.2 Middle managers as intermediaries

Goals, activities, and values set by top management are undoubtedly important for organizational alignment and thus cybersecurity initiatives. Hu et al. (2012) were one of the first to examine how top management can influence cybersecurity compliance behavior of employees. In their study, they focus on the influence cultural values oriented towards rules or goals have on individual cognitive beliefs towards cybersecurity policies. While we will not extensively reiterate the results of the survey, some of the main findings were that top management strongly influences organizational culture, which in turn affects employees' attitudes. However, Hu et al. (2012) also point out that the cybersecurity initiatives by top management may not be visible to lower level employees due to physical and structural distance. Here, the authors refer to Liu et al. (2011), which found that employees are less influenced by removed top executives in large organizations, than by their peers and immediate supervisors.

The middle manager can therefore be an important factor in cyber risk management, as they shorten the distance between top management initiatives and employees. Daud et al. (2018, p. 8) also briefly mention that middle management has been "observed to bridge and serve other levels; top management, technical team and end users". While this topic does not seem to be in the limelight of cybersecurity research, other research fields have given middle managers a greater focus.

Holmemo and Ingvaldsen (2016), in researching lean-implementation, found that middle managers were effectively bypassed in the implementation-process. The authors present two views from the literature on middle managers as change agents: middle managers as

corporate bureaucracy leftovers and "dinosaurs"; and middle managers as strategic "dynamos" (p. 1334). Despite the "dinosaur-view" being the predominant view within the literature, the conclusion of their research was that unless middle managers were involved, enthusiastic top management and successful application of the tools by operational managers were not sufficient. Thus, the transformation process would most likely stall due to lack of coordination and involvement. Despite lean being a divergent topic for this thesis, the findings of Holmemo and Ingvaldsen (2016) are not significantly unrelated, as middle managers are important for implementing initiatives from both top management and the cybersecurity department downwards to their employees and thus leverage alignment.

2.4 From compliance to internalization

2.4.1 Cybersecurity culture

The alignment literature mainly focuses on alignment at a management level. However, according to findings of Safa et al. (2016), organizations fail to achieve successful cybersecurity efforts if they neglect the focus on individuals. Furthermore, the effectiveness of standards and frameworks depend on employees' compliance. Employee's compliances are influenced by factors such as commitment, beliefs, and involvement.

While employees are often viewed as the weakest link in regard to cybersecurity (Hu et al., 2012), more authors are directing their focus towards seeing employees as an important security asset (Da Veiga et al., 2020). In the later years, there has been developed a culture of cybersecurity where the employee recognizes himself as the security and is able to identify threats. Cybersecurity culture is defined by Da Veiga et al. (2020, p. 19) as:

> Information security culture is contextualised to the behaviour of humans in an organisational context to protect information processed by the organisation through compliance with the information security policy and procedures and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives.

Da Veiga et al. (2020) find that there can be a dissonance between employers and employee's efforts to ensure the organization's cybersecurity, because they view the concept of cybersecurity differently. Hence, successful cyber risk management also requires a holistic approach where both employees and management are an active part of cyber risk management.

The operational approach to cyber risk management by Kosub (2015) is aimed to be a more holistic approach than the original PDCA-cycle. This approach includes risk identification, risks assessment and valuation, risk response and risk control objectives, and risk governance and risk culture. Similar to the PDCA-cycle, the first four components should be implemented as a continuous circle, while risk governance and culture, which are in focus, are a subsequent element.

Risk governance and culture are described as "a subsequent organizational element of a holistic cyber management approach, which needs to be continuously maintained and intensified within businesses […]" (Kosub, 2015, p. 622). Within this component, there is a focus on risk awareness among all employees, instructions on IT security and providing regular trainings for all employees, as well as establishing a company-wide risk culture. They also stress the role of management, who should control, supervise, and emphasize cyber risks. Top managers, business and functional managers, system and information

owners, chief information officers, and IT security personnel in particular have to fulfill their roles in order to establish operational risk culture (Kosub, 2015).

Organizational alignment can very simplified be described as a shared purpose, which can be leveraged by organizational culture. However, organizational culture will differ between organizational units, especially in large organizations (Becker et al., 2017). The cultural differences between such units can be described as subcultures, or an already discussed term, organizational silos (Taylor, 2014). According to Taylor (2014), subcultures arise when units find their own successful ways of performing tasks and thus create their own shared purpose.

In large organizations, policies tend to be uniform to encourage a shared approach to security for all members of the organization (Becker et al., 2017). However, misalignment of the "shared purpose" is prone to cause frictions and workarounds. The authors therefore examine policy effectiveness and explore how organizations can engage employees to identify and solve shortcomings of security policies. They discuss the benefits of employee participation in building security policies, and cyber champions' role in enabling participation. Cyber champions are described as "Local representatives who can promote and monitor security policy at a local level, acting as an extension of the company's security management team" (Becker et al., 2017, p. 1).

Becker et al. (2017) base their findings on a survey answered by 600 employees across four business areas (Sales & Services, Operations, Business, and Finance & Professional Services) within an organization. According to the authors, there are three main challenges for effective policies in large organizations. First, non-compliance with policies is common, and employees facing ineffective policies may resort to shadow security. Kirlappos et al. (2014) defines shadow security as workarounds that the official security staff is not aware of and can happen when the security policy undermines organizational productivity. Becker et al. (2017) further adds that the organization's standpoint and values must be clear to the employees, and these values must be reciprocal. That is, the values' power depends on visible evidence that the organization cares and is loyal to the employees. Therefore, cyber champions can only promote policies if they are workable and understood as protection of the organization. Second, organizations must reflect on existing policies before determining the needed cyber champions. Here, the authors are referencing to Pfleeger et al. (2014) and security hygiene. That is workable habits that deliver effective risk management, arguing that this is only achievable when employees are involved in shaping a policy they can comply with. Third, effective security requires a range of different individuals. Their findings suggest that a spectrum of different employees can contribute to effective policies. Those who: follow and promote security policies; question policies; challenge policies through finding alternative solutions; socialize security solutions through engagement with peers; would expect security to justify itself by being a critical part of their productive work.

2.4.2 Improving cybersecurity behavior through influence and change

Cybersecurity culture, as defined by Da Veiga et al. (2020), describes cybersecurity as an embedded part of the individuals behavior. Alshaikh and Adamson (2021) take on a psychological attachment theory by Kelman (1958) to move cybersecurity from simple awareness to sustainable behavioral change. Kelman (1958) includes three processes of attitude change: compliance, identification, and internalization. "Individual behavior and attitude can either be superficial and temporary or result in sustainable change" (Alshaikh & Adamson, 2021, p. 831; Kelman, 1958). Table 1 provides a summary of the theory in

the context of a security awareness program at each level of influence (Alshaikh & Adamson, 2021, p. 835).

Alshaikh and Adamson (2021) research this theory through a case study of Telstra, a leading Australian telecommunication company. Telstra began changing their cybersecurity work in 2014. At that point, the security awareness capabilities were compliance-focused on standards, security policies, and annual compliance training. The cybersecurity responsibilities were laid on IT and the security team. Telstra made changes through shifting their focus from technology to people, establishing both a security influence team and cyber champion network. Cyber champions were recruited through the team, a process which was later automated. That way, the cyber champion network could be scaled up, without increasing the workload of the cyber influencers. One of the main takeaways is that fear-based approaches do not change behavior. The cyber champions were also described as "force multipliers" and were needed to communicate cybersecurity and establish a good relationship between employees from different departments.

Table 1: Levels of influence from Alshaikh and Adamson (2021, p. 835).

Influence level	**Description of cybersecurity awareness**	**Cybersecurity strategies**	**Level and duration of behavior change**
Compliance	Employees follow security policies to gain approval or avoid punishment. Employees will comply if they are being watched (surveillance is the condition of adopting the induced behavior)	Annual mandatory training or ad hoc awareness program that focuses on raising awareness, not influence and change behavior.	Temporary, superficial
Identification	At this level, employees will follow the policies because they want to establish or maintain their relationship with the people who are telling them to do so in this case the security team/the security managers. This is the process of building security culture.	Build effective relationships and trust through the following strategies: Shift the focus from IT security to business enablement. Establish a cybersecurity champion network. Build a positive brand and reputation. Use automation to provide an improved customer experience.	Achieve behavior change.
Internalization	At this level employees follow the security policies because they have the same beliefs and value system with the security team.	Making security more understandable, relatable, and relevant, using the following strategies: Develop creative and innovative awareness methods. Use storytelling and case studies. Relate security issues to employee's personal lives.	Sustainable behavior change.

Compliance level
Compliance is the most common level of influence in organizations. Security awareness programs are primarily driven by industry regulatory requirements and standards. Security policies are followed because employees either want to avoid punishment or to gain approval. Alshaikh and Adamson (2021) discuss why this is the most common level. First, in addition to the challenges of changing behavior, advancement of technologies such as big data analytics, AI and blockchain has entrenched the technological view. Employees trust that technological controls can protect them. Second, employees do not always understand their role in cybersecurity, as IT and security departments are often perceived as the main protectors from cyber-attacks. Employees therefore lack an understanding of security policies and management controls, and security specialists are perceived to be in a policing role. Lastly, limited resources and shortage of specialists in security awareness and behavior change prevent organizations from improving their influence level.

Identification level
Alshaikh and Adamson (2021) provide several strategies for moving from compliance to identification level. These strategies aim to improve the security team's image and build trust between security specialists and employees. The first strategy is to shift focus from IT security to business security. Job performance is an important factor for employees. They are more likely to violate security policies if it hinders their productivity. Violations are viewed as a legitimate means to a desired end. Involving employees in the process of developing policies and controls could improve collaboration and mutual understanding. The second strategy is to establish a cybersecurity champion network. It is impossible for security teams to build culture on their own in large organizations. Cybersecurity has to be a collaborate effort. The last strategy is to build the security team's brand and reputation: In the case of Telstra, the influence team worked together to build a responsive and cohesive security unit. In that way, the security team were not viewed as slow or inconsistent. Furthermore, the influence team enabled the champion network to order three services: (1) training and team briefings; (2) phishing drills; and (3) providing a security operational center team tour.

Internalization level
At this level, employees no longer perform because they have to, but because they have internalized the company's values and beliefs. They perform because the behavior is intrinsically rewarding – they believe it is the right thing to do. To achieve this level, security issues have to be communicated in a relatable and understandable way. Security messages should be personalized, and rules on security behaviors must be actionable and feasible. One strategy for internalization at Telstra is storytelling. "Good stories are shared and retold" (Alshaikh & Adamson, 2021, p. 839). Stories can be used to shape and reinforce employee's values, as they have significant effects on people's minds.

2.4.3 Communication
Communication carries strategies, information, policies and instruction across the organization. According to Gochhayat et al. (2017), literature suggests that communication tends to entertain a meaningful role in the relationship between organizational effectiveness and oraganizational culture. Organizational communication has a positive impact on organizational culture, which in turn increase organizational effectiveness. Organizational communication also provides guidance, sorts out confusion or disagreements and motivates to follow the goals of the organization. Moreover, effective communication is an important factor for alignment (Luftman et al., 2017; Manfreda & Štemberger, 2019). Here, Manfreda and Štemberger (2019) reference to Charoensuk et al. (2014), who furthermore reference to shared domain knowledge. That is, when both

units are learning to understand each other. Effective communication enhances knowledge sharing and thus understanding between business and IT.

In terms of cyber risk management, risk communication is particularly relevant. An organization consists of a number of different individuals, a natural assumption is therefore that different individuals will understand and perceive risk differently. The question is therefore how one can effectively communicate risk. Nurse et al. (2011) highlights the importance of trust and effectiveness in communication of risks. "As such, a risk message that is accurate, specific, presented appropriately and is familiar, is more likely to be trusted and acted on than a message that is to the contrary." (Nurse et al., 2011, p. 61).

The issue of risk communication is very complex because it relies on many factors: how the message is presented; how it is perceived; and the decision-making that comes out of it. Nurse et al. (2011) explain these three elements to risk communication:

1. *The risk message*: What the message consists of, the details of the risk, the complexity of how it is presented, level of required knowledge to understand and the accuracy of the information. An example of this could be a very technical cyber risk which requires significant cybersecurity knowledge to fully understand. A risk message like this would be difficult to understand for someone who does not have knowledge of cybersecurity.
2. *The risk communicator*: How the risk communicator elaborates the risk to the message receiver. This could lead to inconsistencies in how the message is delivered due to different interpretations of the message.
3. *The message receiver*: How the person or people who receive the message perceive and understand the risk that is being presented to them. There are multiple sources of error here, including the recipient´s knowledge, language barriers and beliefs.

Nurse et al. (2011) further presents some recommendations for how cyber risk communication can be improved. First, plan how the risk should be communicated. Second, communicate the risk appropriately to different receivers based on their prerequisites for understanding the message. Third, ensure that the information is clear. Lastly, messages should be communicated in a standard format which is familiar to the receiver, and in a timely fashion.

In our case, it is reasonable to assume that the cyber professionals have a better understanding of cyber risks than the middle managers who don´t work within cybersecurity. When it comes to cyber risk, it is often the cyber professional who is the risk communicator and other people in the organization who are the message receivers. How the message is elaborated and how the cyber professional communicates it therefore plays a large role in how the middle managers interpret and act on it. Understanding how one can communicate risk as best as possible is hereby important in facilitating organizational risk management.

3 Methodological approach

We have chosen a single case study with embedded units to answer our research question:

> *What are the most important building blocks for achieving alignment between middle managers and cyber professionals?*

Such case studies with embedded units can be described as looking at subunits within a larger case (Yin, 2018). The subunits in this case are the cyber professionals and middle managers. The data from these subunits can then be analyzed within, between and across (Ayres et al., 2003). This analyzing strategy will be further explained in 3.3. Data analysis.

The purpose of a case study is to understand a situation in greater depth, and thus the focus is one or few cases within their natural setting (Leedy & Ormrod, 2021). Researchers should consider a case study design when a) one wish to answer "how" and "why"; b) the behavior of those involved cannot be manipulated; c) you believe the contextual conditions are relevant to the phenomenon of the study; or d) the boundaries between phenomenon and context are not clear (Yin, 2018).

Case study research is a part of the qualitative research field. There are several advantages of a qualitative approach. According to Leedy and Ormrod (2021), qualitative methods can give us initial insights, reveal possible complex processes and systems, develop new concepts or theoretical perspectives, uncover key problems within the phenomenon and means to judge the effectiveness of practices.

Cybersecurity in the maritime domain is a growing research field. According to a systematic literature review by Bolbot et al. (2022), risk calculation, acceptance criteria and technical controls are some the dominating research directions within the field. Larsen and Lund (2021) argue that maritime cybersecurity goes beyond technological aspects, and there is a lack of focus on human resources in cybersecurity within the maritime industry. Furthermore, as technological developments and cybersecurity are moving at an escalating speed, cybersecurity in the maritime domain is a highly contemporary phenomenon. Based on the case and research question, we believe that reducing the findings to numerical values will be counterproductive. Therefore, a qualitative approach is best fitted for our method of data collection.

3.1 Limitations and qualitative measures

3.1.1 Limitations of the study

Case studies have some common limitations. Especially single case-studies can lack scientific rigor and thus have less generalizable results. They are difficult to replicate and time-consuming. Additionally, case studies are subject to researcher's own biases. Our knowledge of the maritime industry is based on academic literature and discussions with individuals within the field. Researchers in unknown fields can be prone to influence from others. Therefore, we, as novice researchers, must be aware of our own biases.

Single case-studies are seldom directly generalizable. This thesis has a narrow context and case; a technology provider within the maritime industry. The phenomenon, cybersecurity in a technology organization, is neither new nor unexplored. Some of the findings can be

transferred or generalized based on the characteristics of the case-organization – it is a highly complex, technology-intensive organization. However, it is important to bear in mind that we research a single, Norwegian-based case. We therefore lack an international aspect, especially in terms of industry practices and management. Commonly known as "the Norwegian model". These features must be considered if one was to transfer the findings to other organizations and countries.

In addition, the research question was changed after we had begun interviewing subjects. In order to maintain some consistencies in our findings, the interview guide was not subject to considerable changes. The result of the data collection was therefore more general than originally desired. The piloting research question also set a somewhat different direction for our preliminary literature search. The theoretical background was therefore built in tandem with the first few interviews.

Due to both challenges in terms of theory, but also the contemporary characteristics of our research, we have used literature from other research fields and contexts. Therefore, concepts, terms and models have been translated into the context of the thesis. While this is not necessarily a weakness, and rather the process of academic research, this is a pitfall we have had in mind while writing this thesis.

3.1.2 Qualitative measures

Reliability and validity are often associated with accuracy, stability and consistency in quantitative methods, and has therefore been rejected in qualitative research (Morse et al., 2002). Golafshani (2003) on the other hand, describe validity and reliability as rigor, quality and trustworthiness and contend that the terms are still applicable for qualitative research. Noble and Smith (2015) provide a similar description. According to the authors, the terms are applicable where reliability describes a consistency within the analytical procedures and validity refers to the application and integration of the methods, and how precise the findings reflect the data. In addition to trustworthiness, they suggest the term credibility. These terms, along with confirmability, are also used as a translation of internal validity in Leedy and Ormrod (2021). With this in mind, we will shortly present some qualitative measures.

Construct validity is to what extent the assessment strategy identifies correct operational measures (Leedy & Ormrod, 2021; Yin, 2018).

Internal validity mainly seeks to establish a causal relationship (Yin, 2018). As qualitative data can't be quantified in the same manner as quantitative data, establishing a causal relationship is not possible. Internal validity in qualitative research can instead be described as "to which extent the researcher's course of action and findings reflect the purpose of the study and represent reality" (Johannessen et al., 2016, pp. 232, our translation).

External validity is to the extent the findings can be generalized (Yin, 2018). The generalizability within the maritime industry can be discussed, however this is not the intent of the study. Nonetheless, we believe that the results can be generalized to similar organizations and industries. The research's generality is based on whether it succeeds in establishing concepts, interpretations and descriptions that are useful for additional areas and cases (Johannessen et al., 2016).

Reliability in qualitative research can be achieved through reproducibility, accuracy and stability (Hayes & Krippendorff, 2007). Researchers should strive to position their work to

reflect the concern of reliability (Yin, 2018). This includes a transparent and thorough description of the case and research process.

3.1.3 Ethical considerations

The paper *Ethical Considerations in Maritime Cybersecurity Research* by Oruc (2022) offers ethical recommendations to guide researchers studying maritime cybersecurity. According to Oruc (2022), maritime cybersecurity research should follow six ethical principles: integrity, professional responsibility, accountability, confidentiality, legality and openness.

Integrity relates to truthfulness and honesty, and the researcher must strive to convey the truth and nothing but the truth (Leedy & Ormrod, 2021; Oruc, 2022). Maintaining integrity includes avoiding fabrication, plagiarism, falsification, identifying biases and limitations, transparency, and confidentiality to protect privacy.

The principles of professional responsibility and legality address a responsibility to familiarize ourselves with national and international maritime culture, and being up to date on local rules and regulations (Oruc, 2022). In addition, we shall follow all requirements stipulated in signed agreements. One important notion in this regard is to neither exploit nor allow exploitation of detected vulnerabilities. As studies have the potential to discover cyber vulnerabilities, incidents should not be shared without permissions for related parties, and results of tests such as penetration tests should not be published. Furthermore, personal data of staff associated with the research should be strictly protected.

The methodology should aim to minimize all potential risks, including safety hazards and environmental damage. As this study will be conducted through digital interviews, there is no risk of physical or environmental damage. However, a sentiment on accountability is that researchers are responsible for explaining and defending the study, including method and findings.

Researchers should maximize the benefits for the maritime industry, and always consider the industry's well-being. Openness improves trust and credibility, and methods, tools and findings should be described clearly. If data or tools are developed, they should be shared through fitting platforms. While disclosure of cyber vulnerabilities can be a risk to the industry, information sharing can also improve cyber resilience in the maritime industry.

3.2 Selection of participant and data collection

Qualitative research requires "collecting a series of intense, full, and saturated descriptions of the experience under investigation" (Polkinghorne, 2005, p. 139). Polkinghorne (2005) describes the unit of qualitative search as experience. Participants are chosen based on the ability to provide a substantial contribution. Whether the contribution is substantial or not depends on the participant's experiences. The researcher therefore has to choose participants who are both willing and capable of sharing adequate experiences. In addition, multiple participants will deepen the understanding of the phenomenon by presenting different perspectives about the experience and thus contrasting views the researcher can compare. In this sense, this serves as a form of triangulation, according to Polkinghorne (2005).

While qualitative studies use a smaller number of participants than quantitative research, the sufficient or correct number of participants is seldom clear. Dworkin (2012) provide a commentary on the question of "how many?". Albeit this commentary is directed towards

researchers using grounded theory and in-depth interviews, the author provides a relevant comment on data saturation. Saturation is "the point at which the data collection process no longer offers any new or relevant data (Dworkin, 2012, p. 1). At the same time, there are several factors influencing the saturation and some of them are out of the researcher's control. For example, monetary resources, time and the researcher's ability to determine if one has actually reached saturation. We, as students, are of course limited by our experience and knowledge in this case, especially regarding the maritime domain. This factor strongly influenced our selection strategy.

Our initial strategy was purposive sampling. In purposive sampling, the goal is to find the individuals who can yield the most information about our topic (Leedy & Ormrod, 2021). However, we faced some constraints. As students, our access to and knowledge of key persons within the organization is limited. We have therefore been dependent on convenience sampling and snowball sampling (Leedy & Ormrod, 2021).

This resulted in five middle managers from various areas of the organization and three cyber professionals. The variety of middle managers gave us a range of experiences, which we believe reflect the diversity one typically finds within large organizations. As the cybersecurity department was only established a couple of years ago and has a dozen employees, we are satisfied with number of cyber professionals. The selection and grouping of participants are presented in Table 2 below and is anonymized according to our data handling plan.

Table 2: Overview of participants

Participant number	Role within the organization	Length of interview	Time of interview
Middle managers			
#1	Product line manager	50 minutes	April – 2023
#3	Supply manager	50 minutes	April – 2023
#4	Product line manger	55 minutes	April – 2023
#5	Sales manager	55 minutes	May – 2023
#8	Manager within digital controls	60 minutes	May – 2023
Cyber professionals			
#2	Cybersecurity leader	55 minutes	April – 2023
#6	Cybersecurity engineer	55 minutes	May – 2023
#7	Compliance cybersecurity specialist	55 minutes	May – 2023

Data in qualitative studies is usually derived from multiple sources, such as observations, interviews and documents (Leedy & Ormrod, 2021). In case studies, interviews are one of the most important forms of data collection because they give the researcher deep insight in the phenomenon being studied (Yin, 2018). We have chosen one-on-one interviews with a semi-structured interview guide based on our research question. After each conducted interview, we transcribed them in intelligent verbatim. That is, leaving out pauses and false starts.

An interview guide directs the conversation towards the research topic and increase the odds for later comparison of respondent's answers (Kallio et al., 2016; Leedy & Ormrod, 2021). The quality of the interview guide will affect the implementation and result of

collected data, hence it is important that the questions are formulated to achieve the richest possible data (Kallio et al., 2016). Moreover, a semi-structured interview facilitates follow-up questions and conversation, and thus opens for the participants perspectives, thoughts, and experiences.

The interview guide was structured according to a few selected main themes: cybersecurity, risk management and autonomous vessels. Attentive readers will notice that the latter theme, autonomous vessels, derives from our research question. This was because the interview guide was based on a preliminary research question. A small digression on this note, autonomous vessels gave us a context of cybersecurity at sea due to increased connectivity. In addition to the main themes, we had some questions at hand if there was time to elaborate further. All but one of the interview objects were Norwegian, the interview guide was therefore written in both English and Norwegian.

The first half of the participants were interviewed over a period of three weeks. It took a couple of more weeks to recruit the second half of the participants. These were then interviewed over the course of one week. Despite the prolonged time frame, there were no major changes in the interview guide. All but one of the interviews were conducted in Norwegian. All interviews were carried out digitally, over Microsoft Teams. This was due to the geographical location of the interview objects. Besides a maximum time of 60 minutes per interviews, we had no restrictions on the time spent answering our questions. This was to gather as much information as possible and let the interview objects elaborate freely on the relevant topics. Most of the time, we had time to ask additional questions.

All participants received a short information letter prior to the interviews, which also included a declaration of consent to being interviewed and recorded. Each interview began with a repetition of the declaration of consent, especially to being recorded, and our research question. We then introduced ourselves before following the interview guide throughout the interview. The participants were asked to introduce themselves with some basic background information, before they were asked questions regarding the three main themes: cybersecurity, risk management and autonomous vessels.

The interview guide worked well, in our opinion. However, we do believe that digital interviews somewhat limits both researchers and participants. According to Van Zeeland et al. (2021), online interviews can have negative effects such as difficulty in asking follow-up questions, misinterpretation of pauses, self-consciousness and lead interviewees to be more cautious when discussing certain topics. While the participants gave extensive answers most of the time, they were also to some extent general. We cannot conclude if this was because of the interview guide itself or the digital setting, but it is still important to bear in mind.

In addition to performing interviews, we also performed research of the case-organization through open sources such as annual reports, presentations and articles on their website. Through this research, we found that the case-organization is certified according to ISO45001, ISO9001, ISO14001, and ISO27001.

3.3 Data analysis

The data analysis is a crucial part of qualitative research and the analysis often involves codification of the data material (Leedy & Ormrod, 2021). Coding is a crucial aspect of empirical analysis (Basit, 2003). Codes can either be created a *priori* or emerge as the data is reviewed (Basit, 2003; Blair, 2015). The latter is also known as an inductive method.

Codification can, however, strip the richness from the individual experiences and fail to capture individual uniqueness within cases (Ayres et al., 2003). An approach that seeks to capture both the unique cases and the experiences that are relevant across the cases are the *within-case and cross-case* strategy. Ayres et al. (2003) present three different approaches to this strategy, with the aim of producing contextually grounded, generalizable findings. Generalizability in their article refers to the applicability of findings beyond the research sample. Themes that occur both individually and across the sample are more likely to be generalizable. Therefore, researchers must be aware of and distinguish between individual experiences that are exclusive to certain participants and those that are relevant to all participants.

For the within-case and cross-case strategy to fit our research design, we will lift the within-case analysis from individual level to group level. This denotes that cyber professionals will be viewed as one group, and middle managers will be viewed as another group. We implement this modification because it would not be particularly beneficial to analyze extensively within each individual case based on our research question. Individual differences will be considered when analyzing our findings, as we realize managers and cyber professionals have different positions and functions within the case-organization. Presumably, this will particularly apply to middle managers, as the case-organization is a large organization who different services and products. Nonetheless, the focus will be within the two groups, which will then be further analyzed as a cross-case.

The strategy will be performed in a series of steps, as shown in Table 3. There are a couple of things we would like to point out regarding these steps. First, most of these steps are a process that will not occur in written format in the thesis. Second, the table is predominantly based on the steps by Ayres et al. (2003), but we have added the level-column. 1 and 2 will be carried out at an individual level because we will perform individual interviews, the next steps are performed at a group level.

Table 3: Within-case and cross-case analyze, based on Ayres et al. (2003, p. 4)

Step	Strategy	Analytical focus	Level	Product
1	Review interview transcripts	Within all cases	Individual	Sense of situation for each participant
2	Immersion in each interview	Within all cases	Individual	Identification of significant statements, repetitions, focus
3	Comparison of significant findings	Within and across all cases	Group	Common themes / categories
4	Reconnection to original context	Within and across all cases	Group	Validation of findings
5	Intuiting, critical reflection	Within and across all cases	Group	Common and contradicting themes and categories, structure and summary

3.4 A case study of an organization in an exposed industry

The rapid digitalization of existing services and introduction to new technology has increased the attack surface of the maritime industry (Meland et al., 2021). Both the number of attacks and the width of the attack surface has increased the recent years. According to Meland et al. (2021), most of the attacks are economically motivated, but there are also more sophisticated attacks where the goal is espionage and disruption. A few years ago, A.P. Møller-Maersk was the victim of one of the most devastating cyberattacks in history; the ransomware NotPetya (Greenberg, 2018). As many others, Møller-Maersk was not the original target for the attack but suffered a major economic loss. Several of the company's ports were brought to a halt due to closed gates and frozen cranes. Six years later, the suffering of Møller-Maersk may be a faint memory for many actors in the maritime industry, but cyber threats are not becoming less prevalent.

Our chosen case is a large maritime technology provider based in Norway, with multiple offices in different parts of the world. It is therefore a global actor within the maritime industry. The organization was founded several decades ago, but their cybersecurity team was recently established. They, as many other maritime actors, are experiencing an increasing need for cybersecurity. As with the majority of maritime industry, they are exposed to international competition, but also international threat actors. Investigating cybersecurity in a maritime organization is therefore highly interesting and relevant.

The case-organization is one of many actors developing the field of autonomous shipping. Autonomous shipping is viewed as a necessary development to cope with future shortage of workforce (Divine Caesar et al., 2021). With autonomous shipping, more workstations can be moved from sea to shore, and make the maritime industry more attractive for the generations to come. Some might describe autonomous shipping as the epitome of shipping, but it also presents a new set of cyber challenges. Autonomous shipping implies an increased integration of operational technology (OT) and information technology (IT), and thus an increased risk environment (BIMCO, 2021). Remotely piloted and autonomous marine vessels are furthermore especially reliant on navigational systems (Androjna et al., 2020; Ben Farah et al., 2022).

According to The Danish Cyber and Information Security strategy for the maritime sector, 2019 – 2022, there are three main vulnerabilities within the maritime industry: lack of timely response to technical vulnerabilities; no process in place for upgrades; and securing critical systems. Thousands of ships sailing the seas today have so-called legacy systems onboard which historically have been offline. Today, the connection is increasing, and systems are becoming more complex, but many maritime actors can be described as conservative and old-fashioned. The United Kingdom Department for Transport lists six motivations for cyber-attack on a ship system in an IET standard code of practice for Cybersecurity for Ships (Department of transport UK, 2017). The actors range from low-level criminals to terrorists and state sponsored actors. Their goals are vandalism, economical or physical disruption or disruption of infrastructure and denial of use.

4 Empirical findings

As described in chapter 3.3 Data analysis, we have performed a within-case and cross-case analysis between the two groups cyber professionals and middle managers. The analysis is based on findings from digital interviews. The results presented in this chapter are the product of step one to five in Table 3. To summarize this process for the reader, we have first transcribed and immersed ourselves in each interview before comparing and validating significant findings between the two groups. These findings have been reflected upon and categorized, as shown in Table 4.

The participants were not given any restrictions in time spent answering our questions. Initially, we let the participants speak freely, but noticed that we occasionally had to steer the conversation back to relevant topics. We would like to emphasize that because the interviews were conducted digitally, it was more difficult to interpret why participants twisted their answers into other topics or gave very short answers. However, there was a noticeable pattern that respondents who seemed confident when answering the given question gave more precise answers, while those who seemed insecure tended to drift away from the original topic. For instance, we noticed differences in middle managers being confident when talking about cybersecurity and those who were not.

The findings, summarized in Table 4, show that there are misalignments between middle managers and cyber professionals across all categories. There is a contrast between middle managers' and cyber professionals' views on cyber risk management and also on what is sufficient risk communication and cybersecurity compliance and awareness.

It is evident that the business-orientation infuses the middle managers' approach to cybersecurity. First, they have a very pragmatic way of looking at risks – direct results and consequences. Second, risks are to be handled by the right person, that includes cyber risks. On one side, this can be because of time management. Middle managers cannot handle every risk the organization is exposed to. They therefore focus on the risks that are immediately relevant to their line of work. For example, safety risks are important for those who deliver physical products that can potentially cause physical harm if they fail, while supply risks are important for those who work directly with supply chains. One the other side, this can also be due to knowledge. Those who have domain knowledge of a certain product should also handle its risks. Third, their main focus on challenges related to cybersecurity is policies that cause friction and can hamper workflows.

Cyber risks are on the other hand all but direct results and consequences. This could be one of the main reasons why cyber professionals had to translate their cyber risk messages from cyber risk to business risk for the middle managers to understand. However, simplifying or translating messages can lose their original meaning. As a result, middle managers or others would not understand the complete risks and why they occur. From this, it is clear they lack a coherent taxonomy and thus face communication challenges. By increasing the middle managers' knowledge, they will gain a better understanding of cybersecurity terms and risks. In turn, middle managers are likely to advance their risk awareness and ease the communication between cyber professionals and middle managers.

Table 4: Summary of findings

Group Theme	Middle managers	Cyber professionals
Cyber risk management	Act as policy messengers, but not enforcers	Cyber risk management cover compliance and prevention of risk
	Cyber risks are and should be managed by cyber professionals	Cybersecurity spans across the organization
	Trust in cyber professionals and technical controls	Transferring ownership is important, but not all risks are shared
	Better understanding of risk management related to safety and contingency, including cyber risks causing physical harm	Approaches to cyber risks are too narrow and siloed
	Ineffective policies cause friction	Still viewed as a tick box exercise, should be included earlier in the process
	Customer-oriented	Customer-oriented
Cybersecurity compliance and awareness	Compliance-focused	Awareness is generic
	E-learning courses	Need for cyber skills development – tailored training
	Awareness is more important than training	Need for developing a brand for the cyber team
		Internalization of cybersecurity at all levels is the ideal situation
Risk communication	Business risk in focus	Risks are articulated in business terms, avoiding technical jargon
	Content with internal communications	Lack of coherent taxonomy and shared domain knowledge
		Importance of building a relationship

4.1 Cyber risk management

In our preliminary research on the case-organization, we found that the organization is ISO 27001-certified. This is a commonly used cyber risk framework, but the certification was not mentioned by any of the participants. This can be due to the maturity of cybersecurity in the organization. The cyber professionals gave focus to cybersecurity as an immature domain within the maritime industry. One described the organization as "just getting off from the ground". Another gave examples of requirements that as of now are based on prevention, but to stop the real actors, you need to detect, respond, and recover as well.

However, some of the participants gave us answers that involved some elements of typical PDCA-activities. According to the cybersecurity leader, a lot of his time is used to communicate to top management to assure that they understand the cyber risks and top management is furthermore always the one who decides risk appetite. Both the work and

accepted risk must be grounded in top management. In addition, they had to communicate the direction they are working in and what it would mean for certain tasks within the organization.

Middle managers told us they communicated policies and courses from top management, which are also elements of the PDCA-cycle. For instance, when asked about cyber culture, one participant answered:

> We get very pushed on it [cybersecurity] by IT and the organization, and you could say that the only thing I do is that when new courses come out, I make sure to push my employees to take them – but I may not be very good at talking a lot about it and such.
>
> *-Participant #3, Supply manager*

Risk assessments and aggregating risk upwards seemed to be an established way of working with risks. According to one middle manager it was an expectation to manage based on risks, and to have control of risks within your area of work. However, all the middle managers were unanimous that cyber risk assessments are the responsibility of the IT or cybersecurity department, project leaders or product owners. According to one cyber professional, risk assessments are not something one would necessarily share with employees. In many cases, risks and mitigations will only be relevant to some, or it is too sensitive to be "broadcasted" to the entire organization.

When we dug further into who gets insight to the risk assessments and mitigation plans, we found that those who do not have a direct influence or responsibilities are excluded. However, the middle managers did not seem to view this as an issue. They trusted that those who are responsible will take that responsibility, that included cybersecurity.

> We trust [the organization] in general, with the big IT departments and cybersecurity products, that they are up and running. We use [the systems] with limited access and so on. We have not considered everything surrounding it [risk assessments] in particular.
>
> *-Participant #5, Sales manager*

At the same time, according to one cyber professional, they were often involved late in the process and described themselves as a "tick box exercise". Preferably, they wanted to be included in it as much as possible.

> I would say the security lead or the security responsible should also be part of all the system design reviews, system discussions, everything. But we are not, at the moment at least. So, we are still a more a side-sort-of-thing where we just come and do assessment on the side without much involvement during the system discussion. But that has to change.
>
> *-Participant #7, Compliance cybersecurity specialist*

Based on these findings, there seems to be a strong top-down approach to cyber risk management. However, the importance of transferring ownership was also brought up by the cyber professionals. One said that it is essential that processes from top-down are incorporated in the rest of the organization.

> What is important, is to ensure that others can take part in the interpretation and breakdown of the requirements that set guidelines for how to work.
>
> *-Participant #2, Cybersecurity leader*

A means for transferring ownership was using key persons, so-called "cyber champions". When asked to elaborate, he described the champion as someone with domain knowledge, who understands the need for cybersecurity and can communicate with cyber

professionals. In addition, he mentioned that they only have success with champions to the extent where the champion is motivated and have on-the-job training with cyber related tasks. Few of the middle managers had heard about cyber champions. One manager told us there were champions in other areas, but not cyber specifically. He did, however, have a champion within autonomous operations in his group, who according to the middle manager was close to a cyber champion.

> He can bring the right persons to discuss this [cybersecruity] in meetings. He is no expert, but there are certain flags that are raised more quickly with him than with others.
>
> *-Participant #8, Manager within digital controls*

While there was an agreement that cyber champions can work very well, a cyber professional expressed concerns in terms of capacity. For someone to become an operational cyber champion, he or she must be enabled.

> If you're just saying, 'OK, you are [a cyber champion], you have your full time job but on top of that you're going to be a cybersecurity champion' […] Enable them, provide them the opportunity, provide them the time and resources they need.
>
> *-Participant #8, Manager within digital controls*

4.2 Business-orientation

A common observation among the answers from middle managers is the reference to business risk when asked about risk management. Those who had some sort of leadership responsibility all acknowledged that risk management efforts should be grounded in business risk. From a business risk standpoint, the foundation for managing risks should be laid based on the most critical interests of the business - profitability and compliance:

> A risk that is perceived as very large within a project can be carried upwards and assessed as a big problem, a 'red flag'. But when assessed higher up in the hierarchy and seen holistically for the company, the cost of 8 million for example, makes it a small risk in the bigger picture. It must be managed, but you need to do it at the right 'level'.
>
> *-Participant #4, Product line manager*

We realized early that the middle managers' risk-orientation was clearly linked to their line of work. For instance, a product line manager of physical systems was concerned for safety, while the supply manager was mostly concerned for contingency risks:

> Another thing within risk management that we are working a lot on now, because workforce is a scarce resource right now, is to ensure that you have the competence where you [workers] can cover each other if one gets sick or leaves the company. You always want to have a 'next-in-line' who can step in and take over the tasks. This is a type of risk management that we work with in my organization because you are so dependent on having competence on systems and products.
>
> *-Participant #3, Supply manager*

It is not surprising that tangible risks such as safety risks are more comprehensible and viewed as more important. One participant discussed the need to protect intellectual property rights, which can be translated to business risk, but quickly came back to the safety aspect.

> Our products are built up over a long period of time […] To lose everything in a cyber attack is scary too. But the biggest risk is loss of life, environment or equipment.
>
> *-Participant #8, Manager within digital controls*

At the same time, there was also a concern for safety due to technical requirements. One middle manager expressed a worry for technical requirements that people cannot handle. He gave us an example of a requirement from the International Maritime Organization (IMO). They had to change all passwords on a satellite communication system every third month. This resulted in thirty to forty thousand passwords that had to be swapped every third month. In addition, there were hundreds of people who needed access to these passwords. He then put this in the context of an emergency:

> You don't want to put in a password in a security situation in order to push the emergency stop-button or similar. Then it is physical safety versus cybersecurity.
>
> *-Participant #8, Manager within digital controls*

On the other hand, cyber risks were also described as a part of the safety work. One product line manager told us that most cyber incidents could be handled as safety incidents. This manager in particular was responsible of several physical products, both automatic and manual. When describing his employees, he told us:

> I can't speak for everyone, but I think most of them feel a responsibility. I think one can take some shortcuts if you have a customer who is nagging, you have limited time or other things that affect you. But most of them want to protect themselves, the equipment and the company.
>
> *-Participant #1, Product line manager*

Here, the notion of the customer is interesting. Both middle managers and cyber professionals refer to the role of the customer regarding cybersecurity. It goes without saying that customers are an important part of business. One respondent narrates it as a case of "to be or not to be" for many customers, while others do not care for cybersecurity.

> Our products has to be sufficiently secure and the customers has to be satisfied. […] Our customers can't operate if we are not sufficiently secure.
>
> *-Participant #2, cybersecurity leader*

There is also an aspect of what the customer can afford in terms of service on systems connected to the internet and the requirements the customer has. One cyber professional told us that middle managers were more open to discuss cybersecurity if they experienced pressure from customers, but at the same time, equipment with higher levels of security will become more expensive. Therefore, it was a question of what the customer is willing to pay for. Another cyber professional stated that customers did not want to pay for more than what was necessary to fulfill certain requirements or certifications.

4.3 Cybersecurity compliance and awareness

Most of the middle managers seemed to understand the importance of cybersecurity, and they had some basic principles in their everyday work. Every middle manager was also very clear that they follow the organization's guidelines and policies on cybersecurity. It was notable that their attitude towards cybersecurity was rooted in the organization's policies, and not as an internalized part of their work.

It was also evident that some of the work was viewed as, in lack of a better word, a hassle. Several mention restrictions within systems that may prohibit them from working as effectively as they want to. One also expressed that it was unpleasant to always have in the back of your mind that there are malicious actors out there.

> I don't think we should not do anything with it [cyber risks], but it would of course be better if we didn't need to think those kind of thoughts.

-Participant #3, Supply manager

However, we did not get the impression that there was some kind of fear-based culture regarding compliance. When asked questions of how the organization makes sure that employees follow cybersecurity policies, most middle managers focused on basic compliance. They do not have regimes for checking compliance, but there is an expectation of following the given policies. A middle manager stated:

> There is no one running after you, but there are limitations in the IT-system […] There is a combination of wanting to protect oneself, and routines and processes within the system you have to comply to.

-Participant #1, Product line manager

Furthermore, we are given the impression that the middle managers' cybersecurity skills are also based on these basic requirements, for example using two-factor authentication and not using public networks. According to the cyber professionals, the organization is only at an awareness level. The reason for this is that awareness can be made generic, while you will need context driven training because of differences between domains. We also noticed that the cyber professionals saw the training they had today as awareness.

> Awareness is just generic cybersecurity […] We can provide awareness to literally everyone […] Whereas the training side, at least in my view, we want to tailor it to a more context driven training.

-Participant #7, Compliance cybersecurity specialist

Generic cybersecurity is typically what the middle manager described as their active cybersecurity work – use two-factor, VPN and not click on links. The training was described by middle managers as different mandatory e-learning courses sent from "higher-ups" or the IT department. One of the middle managers was both very aware of the courses and brought the courses up in meetings if someone had not taken a course. He also described the courses in great level of detail. Generally, the courses contained information, questions, and some small video clips. The video clips were described as especially helpful.

> They [the video clips] will pinpoint what you should be looking for. And it has been very helpful, because you can typically see the use of upper and lower case letters [in fake e-mails]. Then you get an idea, so you take a second look at things like that.

-Participant #5, Sales manager

This is a very clear example of courses fostering awareness. Furthermore, a different middle manager believes the awareness is more important than the training itself. This is because the information is updated and reminds people of best practices. A somewhat insignificant, but still illustrative finding, is that the respondents we interviewed during the same period mentioned fake Linked-in profiles. Showcasing an example that it is the information you receive last that you remember best.

While not asked to further elaborate on these courses, we can assume that different departments and product lines receive different courses, based on the nature of their work.

This could be why one manager describes awareness, or information, as more important than training, while another middle manager reflects on direct connections between the training and everyday work.

In addition, the cyber professionals emphasized that a part of their awareness work was making themselves visible. They are currently facing a challenge concerning people who still do not know who they are. Demands from customers were briefly mentioned, and those who do not experience such demands do not have security on top of their agenda.

> So then we have to explain to them, OK, security is more like an onion in that you have to go thorugh layer after layer, and then you have to provide security at every layer possible […] So then they start to slowly see the point.
>
> *-Participant #7, Compliance cybersecurity specialist*

This process was not explained as black and white, and sometimes you had to give middle managers and the like time - maybe even let them make some mistakes before they realize that cybersecurity is needed.

> There are a small number who are not fully convinced. They still believe you can just build a [fire] wall around their products. Usually they just need some time for themselves and maybe even learn from their own mistakes from time to time.
>
> *-Participant #6, Cybersecurity engineer*

One cyber professional stated that employees possess awareness but lack understanding. Without specifying a particular group, he explained that they sometimes must "hold their hand" and walk them through requirements and solutions. He further emphasized that they [the cyber professionals] cannot hold all the knowledge. Additionally, it is an impossible task to fully support every single team within the organization. An ideal situation would be more independent product lines, whereas the security team could monitor and be a supporting function, rather than doing all the work as they do today. Nevertheless, the middle managers did not seem to have the same view.

> I am probably able to understand the overall requirements for our products, and what we have to do at an overall level. Then, those who are specialists [the cyber professionals] must be involved in the dialogue and get it done.
>
> *-Participant #1, Product line manager*

4.3.1 Risk communication

Communication of risk is an important part of risk awareness work. The cyber professionals stressed two challenges that made communication difficult. First, translation of cyber risks to business risks, and second, the size of the company and capacity constraints.

According to the cyber professionals, they often had to translate cyber risks to business risks for the management to understand. For example, if something happens to an autonomous ship, it could cause a reputational risk. One of the professionals further emphasized how non-compliance sometimes is their only means of conviction.

> The first question is 'why should we do this? Our things [products] are not connected to anything. It's isolated' and so on. It is a challenge of somehow convincing them that this is something you need to do, but the only way we can convince as of now is the non-compliance aspect.
>
> *-Participant #7, Compliance cybersecurity specialist*

Non-compliance is also a business risk, as this can prohibit the organization from selling products or be a competitive disadvantage.

Some of the cyber professionals brought up that there was a need for a common language within risk management in the organization. Cyber professionals expressed the importance of communicating precisely, especially in relation to engineers. However, to communicate cyber risks precisely, they felt the need to use cybersecurity terms rather than rephrasing the message to make it easier for others to understand. There are therefore conflicts between how the cyber professionals want to communicate cyber risk in a way which maintains the accuracy and trustworthiness of the message, and the lack of knowledge amongst the recipients.

> If you walk up to someone and point out a concrete vulnerability in a concrete software, they ask 'And so? How can this be exploited?'. And that might be a very good point. It depends on whether the risk is an actual risk, for example damage to people, the environment or economically.
>
> *-Participant #6, Cybersecurity engineer*

On the other hand, middle managers did not discuss these communicative challenges to a great extent. Most of the managers mentioned the organization's internal channels as a means of communicating cyber risks. Our impression was that the middle managers were pleased with the information they received through internal channels.

Due to the sheer size of the organization and lack of capacity in both time and people, the cyber professionals often has to communicate digitally. While most communications take place digitally, one cyber professional explained how face-to-face communication is an important tool to ensure that risks are understood and managed properly.

> If we work with upcoming requirements that will entail big changes for some products, then it is simply a matter of sitting in the same room and have a calm chat about what it means and how we can solve it.
>
> *-Participant #6, Cybersecurity engineer*

Another emphasized that meeting physically is important for collaboration and to, over time, build a relationship and work together.

5 Discussion

The upcoming discussion will spring from our research question, which is: *What are the most important building blocks for achieving alignment between middle managers and cyber professionals?*

According to our findings, there are misalignments between cyber professionals and middle managers. These misalignments are likely caused by the business-orientation of middle managers, and how they perceive cybersecurity; it is the responsibility of cyber professionals and IT. Not surprisingly, cyber professionals are more oriented towards cybersecurity challenges.

The lack of cybersecurity knowledge among the middle managers can also cause parts of the misalignment. We already know that knowledge enhance awareness (Safa et al., 2016), and that shared domain knowledge increases effective communication (Charoensuk et al., 2014). It is furthermore reasonable to assume that increased knowledge improves cybersecurity attitudes, because our findings suggest that those with higher cybersecurity knowledge view cybersecurity as more important and valuable.

Although the middle managers would not be expected to possess the same level of knowledge as the cyber professionals, building competencies that go beyond following instructions, and having middle managers perform risk management activities on their own incentives would be beneficial. This would make middle managers function as intermediaries for the cybersecurity efforts, who could contribute to consistency throughout the organization.

Effective communication was furthermore important according to our findings, but a prerequisite for clear communication is the ability to understand the content of the risk message, which requires certain cybersecurity knowledge (Nurse et al., 2011). If the organization emphasized knowledge building within risk management and cybersecurity in general, the findings from our interviews indicate that this would lead to better risk communication.

5.1 Alignment through standardization

As aforementioned, we did not ask the respondents whether they followed a cyber risk management framework, and it was neither brought up by cyber professionals or middle managers. According to the organization's annual report, they are ISO 27001-certified. If such frameworks were integrated as the backbone of cyber risk management, it would be natural to assume that especially cyber professionals would have brought it up unsolicited. On this note, we would like to discuss the use of information security management systems (ISMS), such as the ISO 27001, which is the only certifiable standard in the ISO 27000-series. The system is based on the plan-do-check-act cycle (PDCA-cycle) (Kosub, 2015). As previously mentioned, top management lays the foundation of the system through determining risk appetite and treatment strategies, while lower levels are given certain guidelines which top-level review. In essence, it is similar to an integrated top-down and bottom-up approach (Linkov et al., 2014; Tessier & Otley, 2012).

Frameworks and standards are often used to encourage a shared approach to security (Becker et al., 2017). According to Kure et al. (2018), frameworks are needed to achieve consistent risk management. One assumption is therefore that standardization will leverage alignment throughout the organization because all levels of the organization use the same procedures and policies. Security awareness programs are furthermore primarily driven by industry regulatory requirements and standards (Alshaikh & Adamson, 2021) The benefits of ISMS are that they standardize the processes and make it easier for lower levels to communicate shortcomings and challenges. If the risk management systems are siloed within each department or product line, it can become confusing for both middle management and top management to communicate feedback and measures. Furthermore, clearly stated rules are easier to internalize because they help employees model their behavior (Hu et al., 2012).

On the other hand, according to Kosub (2015), organizations struggle to implement effective cyber risk management despite standards such as ISO 27001. Furthermore, the research by Becker et al. (2017) suggests that security policies cause friction because the same policies and procedures are applied throughout the organization, but the day-to-day reality is different for every individual. Our findings show that there are vast varieties from product line to product line. Although it is a natural assumption that standardization leverage alignment, in cases like our organization, strict standardization can also result in shadow security (Becker et al., 2017; Kirlappos et al., 2014). Shadow security can in turn result in bigger misalignment because how cybersecurity is applied throughout the organization becomes a "black box".

Our findings indicate that cyber risks are not prioritized by top management unless they are translated to business risks. Strategies such as the PDCA-cycles highlight the role of top management. They are the final decision makers in determining which risks the business can and cannot tolerate. Therefore, their role in cyber risk management is important. Yet, cyber risks that are severe in a cybersecurity perspective, may not seem as severe in a business risk perspective. We interpret this as cybersecurity being deprioritized in favor of other more value-creating activities. Especially within large organizations with a high risk-tolerance due to their resources.

According to one cyber professional, while risks should be sent up and then come down to the right person, they sometimes go directly to the relevant person, instead of aggregating the risk upwards. This can be due to experiencing a lack of power in encounters with top management because of the deprioritization of cyber risks. If this is the case, the bottom-up capabilities are likely not optimal. According to Linkov et al. (2014) an integrated top-down and bottom-up management model should facilitate risk management at lower levels, which in turns help to inform decision making at the higher level. The management should therefore strive to empower employees of risk management (Tessier & Otley, 2012).

5.2 From technological controls to people as first line of defense

Cyber risk management in the case-organization is mainly based on compliance with cybersecurity policies and technological controls. This is not an unpredicted finding, as many still view technological control as the primary solution to cyber threats (Alshaikh & Adamson, 2021). On the contrary, only a third of cybersecurity issues can be solved by such controls alone (Cisco, 2018). This misperception implies that there are differences between how organizations perceive cybersecurity measures and mitigations.

Middle managers comply with cybersecurity policies, without putting much thought into it themselves. They trust the cyber professionals' and IT personnels' decisions and requirements. Furthermore, they perceive technology with built in defense mechanisms as sufficient. For instance, they comply with cybersecurity policies in terms of using VPN and two-factor authentication. Cyber professionals on the other hand, were in favor of making the middle managers more self-sufficient and emphasized the importance of building knowledge and engagement around cybersecurity and risk management.

Misaligned expectations can generate inconsistencies in cyber risk management. It was clear that most middle managers trusted that cyber professionals and technological mechanisms would protect them to a higher degree than what was seemingly possible from the cyber professionals' perspective. One can assume that this trust in technology comes from a view of cyber threats as malicious actors who exploit technical vulnerabilities. At the same time, cyber-attacks become more sophisticated and human factors are increasingly being exploited through attack vectors such as social engineering (ENISA, n.d.; Khan et al., 2011). While it is likely that most attempts on social engineering never get past technological controls, one middle manager gave us examples of situations that can be described as attempts of social engineering. He was able to recognize some red flags and reported it, but expressed concerns that this is something we will see more of in the future. Unfortunately, he is right and this stress the call for a shift in focus from technological challenges to social challenges (Li et al., 2019; Soomro et al., 2016; Østby et al., 2020). Consequently, employees can find themselves as the first line of defense against cyber-attacks. This magnifies the importance of increased independence of employees, as they need to recognize themselves as the security and be able to identify threats (Da Veiga et al., 2020).

5.3 From compliance to internalization

It is evident that a change is needed for the organization's cyber risk management to become aligned. Based on the above discussion, cyber risk management from middle managers' view is mainly about technological controls and compliance. While from the cyber professionals' view, there is a need for internalization of cybersecurity behaviors.

Similarly, Kosub (2015) argue that cyber risk management need more than PDCA-cycles, as organizations continue to fail to implement effective cyber risk management. They argue that the complementary components *risk governance and culture* are needed for a holistic cyber management approach. That is, an approach that focuses on more than technological controls and compliance. An important part of risk governance and culture is to establish a company-wide cyber culture. According to Da Veiga et al. (2020), there can be a dissonance between employers and employee's cybersecurity effort, because they view the concept of cybersecurity differently. A company-wide culture could therefore mediate this dissonance. Before continuing this discussion, we would like to take a step back and repeat the definition of cybersecurity culture:

> Information security culture is contextualised to the behaviour of humans in an organisational context to protect information processed by the organisation through compliance with the information security policy and procedures and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives.
>
> (Da Veiga et al., 2020, p. 19)

We do recognize that this definition is towards *information* security culture, but it is applicable to cybersecurity culture as well. The definition refers to a behavior of protecting

the organization through compliance, but also through understanding how to implement these requirements. In a cybersecurity perspective, the protection would also entail protection of assets that can be reached via cyberspace and those that function in cyberspace (Von Solms & Van Niekerk, 2013). The latter will require a deeper understanding of cybersecurity. With this in mind, we will continue our discussion and direct the attention back to cyber professionals and middle managers.

Based on our findings, the case-organization is at a compliance-level. However, the behavior of protection requires more than just compliance. Alshaikh and Adamson (2021) present three levels of influence on behavior: Compliance, identification, and internalization. According to the authors, compliance is the most common level. The reason for this is: 1) technological developments, 2) employees lack an understanding of their own role in cybersecurity and 3) limited resources.

We find all three of these in our findings. First, middle managers rely highly on technological control, most likely because of technological development. Second, there is a gap between how middle managers perceive cybersecurity and how cyber professionals want middle managers to perceive cybersecurity. Hence, middle managers do not understand their role in cybersecurity. Third, cyber professionals are having challenges regarding capacity constraints because they are a small team in a very large organization.

It is already evident that the organization is at a compliance level. At best, in the upper tier of compliance, moving towards the identification level. The reasoning is that the middle managers give no indications of surveillance, rewards or punishment for compliance or non-compliance of security policies. Neither when referring to top management – "there is no one running after you", or to their own employees – "I can't check what my employees do during travels". The lack of enforcement regarding security policies can be linked to how the cyber professionals view security policies. There is a common understanding among them that forcing security policies is a poor strategy. The cyber professionals furthermore expressed that they want the middle managers to become more self-sufficient. The behavior should become more internalized, rather than just compliance-based. This, along with the elements of influence on behavior, compliance, identification, and internalization is illustrated in Figure 3.

While the cyber professionals emphasize the importance of understanding the other party and building a relationship, the middle managers seem less concerned with creating a relationship with the cybersecurity team. This is an important factor of the identification level, and a good relationship has to be established before the organization can achieve the internalization level. Our interpretation of the findings is that they view the security team as a separate silo. A silo in which their only purpose is to ensure compliance and to protect the business – both in terms of financial and reputational risks.

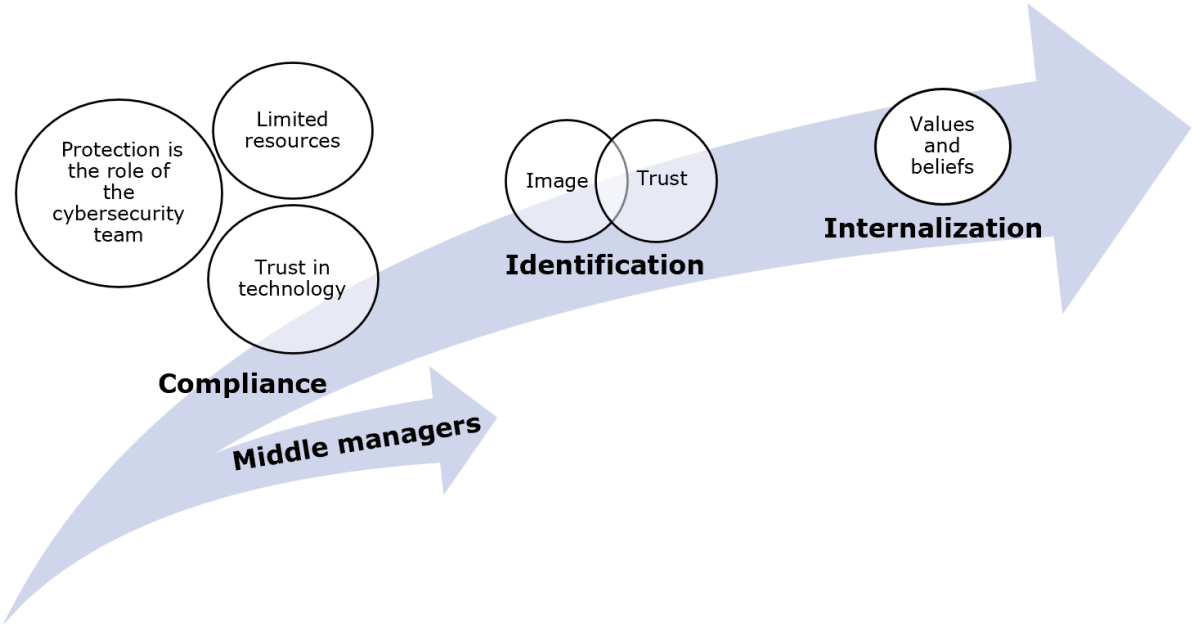
In addition, limited resources can prevent organizations from improving their influence level. Compared to the sheer size of the case-organization, the cybersecurity team is only a small percentage of employees. Therefore, it is especially challenging to make themselves known to the rest of the organization. This is likely to be the reason as to why the middle managers seem to be oblivious to cyber professionals and building a relationship with them. Yet, a good relationship is highly important. According to Manfreda and Štemberger (2019), commitment to a good relationship is one of the most influential items of business-IT relationship.

The cyber professionals emphasized meeting physically and thus make themselves known to employees within the organization. It is likely that meeting in person rather than digitally will improve the brand and reputation of the cyber personnel. Such activities are similar to the strategies for reaching an identification level (Alshaikh & Adamson, 2021). Here, it is clear that the resource constraints are hindering activities that could improve the relationship between middle managers and cyber personnel. However, trust is also an important element of building a relationship. The middle managers express trust in cyber professionals' decision multiple times. This can be a good starting point and foundation for a better relationship. Lastly, Alshaikh and Adamson (2021) also reference changing from cyber risks to business risks to enhance the relationship. This will be discussed later.

Figure 3 is an extended version of Alshaikh and Adamson (2021, p. 831), building on the main components of compliance, identification and internalization. Middle managers are added as a second arrow to illustrate the need for enhancing middle managers' behaviors from compliance to internalization.

First, Figure 3 illustrates the three main reasons for why organizations stay at a compliance level. Based on our empirical findings, the attitudes of middle managers are very similar: They trust technology can provide sufficient security and security is the responsibility of cybersecurity personnel. In addition, it is evident that cyber professionals do not have enough resources to provide sufficient awareness or training. Second, identification can be achieved through a better relationship between cyber professionals and middle managers. This relationship can be improved through branding and trust, in addition to shifting focus from cyber risks to business risks - the latter will be discussed later. Third, if cyber professionals and middle managers can achieve a better relationship, it is possible to achieve an internalization level. At the internalization level, employees perform security activities because they believe it is the right thing to do – cybersecurity behaviors are internalized (Alshaikh & Adamson, 2021). This level can be achieved through better communication and workable security behaviors. Communication and how middle managers can influence their employees to internalize these behaviors will further be discussed below.

Figure 3: Extended version of Alshaikh and Adamson (2021, p. 831)



5.4 Business jargon

According to our findings, most risks must be translated from cyber risks to business risks. The cyber professionals experienced little response from middle managers if cyber risks were presented with appropriate cyber terms. However, translating cyber risks to business risk can be difficult. For instance, it can be impossible to calculate the potential economic loss of a threat before the incident takes place. NotPetya is an example of how one single piece of code can cause damages for billions (Greenberg, 2018). Worst-case scenarios like NotPetya are just that – worst-case scenarios. Businesses can seldom protect themselves from these kinds of threats, and the size of the potential loss becomes impossible to calculate. This illustrates how the severity of a cyber risk cannot always be directly translated into business risk. "Cybersecurity jargon" could therefore be needed to properly communicate the cyber risk.

It is apparent that translation of cyber risks to business risks causes some communicative challenges, at least from the cyber professionals' perspective. As they are a small team, they have to learn a multitude of different languages and jargons in order to get their message across. The literature on the other side, does not discuss these challenges and is adamant that communication should be in "business jargon" (Alshaikh & Adamson, 2021; Manfreda & Štemberger, 2019; Preston & Karahanna, 2009). This notion places the responsibility in the cybersecurity personnel's hands, despite obvious resource constraints such as short-staffed cybersecurity teams.

The skewness of responsibility in terms of communication is likely to hamper effective communication. As communication is an important construct for sharing ideas, information and knowledge, and furthermore can nurture a mutual understanding and trusting relationship between business and IT (Luftman et al., 2017). To leverage these challenges, the focus should be turned to shared domain knowledge. Shared domain knowledge is when *both* units learn to understand each other (Charoensuk et al., 2014). Business and IT skills development are also constructs for better alignment. Enhanced knowledge will therefore increase communication and thus alignment. Consequently, effective communication leads to effective cyber risk management, *both* cyber professionals and middle managers should therefore work to enhance their knowledge.

5.5 Cyber champions – modern day influencers

According to our findings, the organization has champions in some areas, but not within cybersecurity. We got the impression that this was something the organization was working on, but there was some discourse between the cyber professionals. We would therefore like to elaborate on that discussion.

The cybersecurity leader described cyber champions as key persons who have domain knowledge, can communicate with cyber professionals, and understands the needs for cybersecurity. On the other hand, another cyber professional expressed concerns in terms of capacity. Providing cyber champions with needed resources and training is in other words essential for successful implementation.

There are several benefits of cyber champions. First, as they have both domain knowledge and cybersecurity knowledge, they can provide "short-distance assistance" within their department. For instance, if an employee is unsure of a security practice, the champion can provide directions. Second, as they are communicators with the cybersecurity team, they can support mowing ownership of security and risks, making the employees more

self-sufficient. Third, the cyber champion can help middle managers or the security team in mapping the department's security challenges and needs.

Alshaikh and Adamson (2021) suggest a network of cyber champions as one of the strategies for moving from a compliance level to an identification level. Cyber champions are the influencers of cybersecurity and are likely to influence their peers to a higher degree than top management. While top management play an important role for cybersecurity strategies such as the PDCA-cycle, there is evidence that the direct effect top management has on employee attitudes is insignificant (Hu et al., 2012). This could be because employees are more influenced by their peers and immediate supervisors, such as middle managers, than by top management in large organizations (Liu et al., 2011). Furthermore, factors such as commitment and beliefs affect employee's compliance (Safa et al., 2016). The cyber champion can therefore enhance compliance through the influence of his or her peers.

As the case-organization has a range of different product lines and departments, it is clear the one size does not fit all. This is similar to the findings of Becker et al. (2017), where large organizations typically have different cultures and way of working. A cyber champion can here function as "bottom-up" agent who can question policies and negotiate workable solutions (Becker et al., 2017). This way, one can avoid shadow security where the organization is unaware of how the security policies are followed within each product line or department. Furthermore, one cyber professional highlighted the importance of context, both context driven training and context driven compliance. The professionals were willing to engage in discussions regarding requirements, and finding a solution that works for both parties. A cyber champion within a product team could be a key person in these discussions. He or she could provide the cybersecurity team with their context specific challenges and needs, to find that common ground. However, the organization will need capabilities to approach shortcomings in their policies, because cyber champions are highly likely to find gaps in processes and policies.

According to the proposed literature in this thesis, cyber champions are portrayed as the solution of many cyber-related challenges. However, our findings indicate that there are various challenges related to cyber champions within the case-organization. One cyber professional told us they only have success with the cyber champions if they were motivated and had on-the-job training with cyber related tasks. Another cyber professional also emphasized the importance of enabling the cyber champions. He further explained that he views it as an either or. If you are a cyber champion, you have the cyber responsibility in terms of products and services. If you don't have this responsibility, you are not a cyber champion either. As of now, there seems to be no one who has been provided the time and resources to become a cyber champion.

Considering our findings, middle managers and other employees would have a significant amount of trust in a cyber responsible person's assessments. This sort of "blind trust" presents its own set of challenges. Firstly, a cyber champion is not a cyber professional or specialist. He or she could therefore lack the necessary knowledge to perform proper evaluations in some situations. Secondly, there is a chance that no one would be double checking the cyber champion's evaluation and take it as face value. Both the cyber champion, middle managers and cyber professionals must therefore be very aware of this in their work. Lastly, if the cyber champion's view on cybersecurity differs from the cybersecurity team's view, there could continue to be a misalignment in the cyber risk management.

5.6 Middle managers as intermediaries

Our empirical findings suggest that middle managers are unaware that they play an important role in cyber risk management. Furthermore, the siloing of cybersecurity suggests that there are misalignments in expected IT governance. IT governance focus on allocation of authority, processes, and resources (Luftman et al., 2017). Governance should furthermore focus on activities that create a shared purpose. Here, the cybersecurity team is expected to ensure compliance, while middle managers role in cybersecurity, besides being compliant, is non-existent. As immediate supervisors, middle managers have a bigger impact on their employees than top management in many cases (Liu et al., 2011). Employees' view on cyber risk management can therefore be influenced by the skewed relationship between middle managers and cyber professionals. If their immediate supervisors don't take cybersecurity initiatives, why should they?

Every middle manager will probably not become an eager cybersecurity advocate. How involved or motivated they are to support the cyber professionals and their work will most likely depend on motivation and knowledge. Nonetheless, there is a potential for the middle managers to be important intermediaries for cyber risk management. Most of the middle managers told us that they could become better at promoting cybersecurity but did not seem to realize that they have a significant role in the cybersecurity work. However, a couple of managers also focused on facilitating a good discussion or mediate between requirements and employees. Such attitudes can enhance the alignment of cyber risk management within the organization.

First, middle manager can bridge the gap between cyber professionals, top management and employees (Daud et al., 2018). They are the common denominator between these levels. Therefore, as the findings of Holmemo and Ingvaldsen (2016) suggests, effective implementation processes require involvement of middle management. Based on the description of middle management as either dynamos or dinosaurs, it is apparent that top management's success is based on middle management's engagement. For instance, it is debatable whether top management can achieve a certain organizational culture in large organizations without the middle management. The notion of middle managers as dynamos is similar to the description of cyber champions as "force multipliers" by (Alshaikh & Adamson, 2021). This indicates that the desired direction of the middle manager is the direction the employees are likely to go. viewed through this perspective, the middle manager therefore hold a lot of power and will be very important for successful cyber risk management. For instance, they are in a position where they can support their employees through sense-making of security policies. This is a task the cybersecurity team at this stage does not have the capacity to do for every product line or function within the case-organization.

Second, similar to cyber champions, middle managers can function "bottom-up agents" towards both top management and cyber professionals. Due to the small size of the cybersecurity team, it would be impossible to identify where security policies cause friction in every product team or department. As silos occur when teams find their own way of working, such behavior is likely to cause both vertical and horizontal misalignment. According to our findings, the middle manager is aware of workarounds, shadow security, happening. This is an opportunity to pinpoint to the cyber professionals where the policies needed to be made more workable. It is important to bear in mind that cyber professionals will have to maintain their integrity, despite cybersecurity policies sometimes causing

frictions. Removing certain guidelines or skipping certain measures is therefore out of the question in many cases.

Third, adjusting and overcoming shadow security can provide valuable experiences and learning opportunities for both middle managers and cyber professionals. According to Kirlappos et al. (2014), organizations can learn from areas where shadow security occur, and develop effective security policies. This will also enhance alignment with the organizational goals and effectiveness. This is because employees' capacities are enhanced if security solutions are better aligned with their primary tasks.

Lastly, according to our findings, it is apparent that middle managers with higher cybersecurity knowledge also have an increased awareness. This is supported by Safa et al. (2016), who state that cybersecurity knowledge enhances cybersecurity awareness. A concrete example from our findings were middle managers with more knowledge mentioned cybersecurity issues such as social engineering. Attempts of social engineering can be difficult to detect for unaware employees. Consequently, knowledgeable employees will discover red flags faster and more often. With a higher level of awareness, middle manager will also influence their employees to be more aware and thus become a part of the organization's security.

6 Conclusion

The maritime industry is rapidly digitalizing and thus the use of advanced technology is increasing. Yet, cybersecurity is lagging behind and actors in the maritime industry are therefore in need of more efficient cyber risk management to tackle future cybersecurity challenges. In this thesis, we have therefore chosen to explore the research question:

> *What are the most important building blocks for achieving alignment between middle managers and cyber professionals?*

We conducted eight in-depth interviews with three cyber professionals and five middle managers. Through interviews, we found that the responsibility of cybersecurity- and risk management is mainly siloed in the cybersecurity department or similar. In addition, we found that middle managers are highly business-oriented, also when it comes to cybersecurity. This can cause horizontal misalignments as cyber professionals and middle managers have a disparate view on cybersecurity, and vertical misalignments as middle managers are intermediaries between employees, top management, and partly cyber professionals.

Alignment can be defined as a shared purpose and moving in the same direction. We have therefore explored the important building blocks for achieving a shared purpose. We found two main building blocks: organizational cybersecurity culture and shared domain knowledge.

Organizational culture influence both behavior and awareness. Knowledge increases awareness, which in turn enhances effective communication. To improve alignment, one needs shared domain knowledge. Behavior, awareness, and communication are furthermore dependent on the cyber professional or middle manager's knowledge. According to business-IT alignment literature, it is cyber professionals' responsibility to speak in "business jargon". However, to achieve a mutual relationship, which is an important factor for alignment, we argue that middle managers also have to enhance their communication. This way, middle managers and cyber professionals can become more aligned.

6.1 Further research

In our thesis, we have explored how a maritime organization can accomplish more consistent and successful cybersecurity across organizational departments and hierarchies, with emphasis on the interplay between middle managers and cyber professionals. However, future research should expand this emphasis and move both up and down in the organizational hierarchy. Furthermore, we performed a single case study research in Norway, while the maritime domain is a global cluster consisting of a range of different actors: technology providers, shipping companies, fisheries, coastal tourism and more. It would therefore be valuable to perform studies across of these actors and countries.

Building on the findings of this thesis, new research regarding knowledge building and sharing in the maritime domain specifically with their rapidly evolving technology in mind would be interesting. This could either be cybersecurity-oriented or aimed towards other aspects that are of interest in the industry. Additionally, it could be beneficial to establish a way of benchmarking cybersecurity knowledge to ensure that all parts of the organization are at their expected level. Finding ways to increase knowledge of cybersecurity in an

interesting and engaging way is key to carrying it out successfully. As many respondents in our study highlighted, cybersecurity is viewed as extra work that is often conducted on a checklist basis, because of the lack of interest or different prioritizations among employees.

Similarly, additional research can be done on how to establish a common way of communicating cybersecurity – a common language, as mentioned in our study. We did not go into depth on how this can be accomplished, however this is something that future researchers can dig into, perhaps with inspiration from other fields and/or organizations. The intention of establishing a common language is to ensure familiarity with the general cybersecurity terms, for example cyber risks can be communicated more effectively without having to translate important issues in ways that loses content.

References

Alaceva, C., & Rusu, L. (2015). Barriers in achieving business/IT alignment in a large Swedish company: What we have learned? *Computers in human behavior*, *51*, 715-728. https://doi.org/10.1016/j.chb.2014.12.007

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing*, *25*(5), 829-841. https://doi.org/10.1007/s00779-021-01551-2

Althonayan, A., & Andronache, A. (2019). Resiliency under strategic foresight: The effects of cybersecurity management and enterprise risk management alignment. In *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)* (pp. 1-9). IEEE. https://doi.org/10.1109/CyberSA.2019.8899445

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of marine science and engineering*, *8*(10), 1-21. https://doi.org/10.3390/jmse8100776

Aversano, L., Grasso, C., & Tortorella, M. (2012). A literature review of Business/IT Alignment Strategies. *Procedia Technology*, *5*, 462-474.

Ayres, L., Kavanaugh, K., & Knafl, K. A. (2003). Within-case and across-case approaches to qualitative data analysis. *Qualitative health research*, *13*(6), 871-883. https://doi.org/10.1177/1049732303013006008

Basit, T. (2003). Manual or electronic? The role of coding in qualitative data analysis. *Educational research*, *45*(2), 143-154. https://doi.org/10.1080/0013188032000133548

Becker, I., Parkin, S., & Sasse, M. A. (2017). Finding security champions in blends of organisational culture. *Proc. USEC*, *11*. https://doi.org/10.14722/eurousec.2017.23007

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information*, *13*(1), 22. https://doi.org/10.3390/info13010022

BIMCO. (2021). *The Guidelines on Cyber Security Onboard Ships*. The Baltic and International Maritime Council Retrieved from https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Blair, E. (2015). A reflexive exploration of two qualitative data coding techniques. *Journal of Methods and Measurement in the Social Sciences*, *6*(1), 14-29. https://doi.org/10.2458/azu_jmmss.v6i1.18772

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*. https://doi.org/10.1016/j.ijcip.2022.100571

Broussine, M., & Guerrier, Y. (1983). *Surviving as a middle manager*. Routledge.

Charoensuk, S., Wongsurawat, W., & Khang, D. B. (2014). Business-IT Alignment: A practical research approach. *Journal of high technology management research*, *25*(2), 132-147. https://doi.org/10.1016/j.hitech.2014.07.002

Cicek, K., Akyuz, E., & Celik, M. (2019). Future skills requirements analysis in maritime industry. *Procedia Computer Science*, *158*, 270-274. https://doi.org/10.1016/j.procs.2019.09.051

Cisco. (2018). *Cisco 2018 Annual Cybersecurity Report*. https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *computers & security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: can

cooperation promote compliance in organisations? *International Journal of Business & Society*, *19*(1). http://www.ijbs.unimas.my/images/repository/pdf/Vol19-no1-paper11.pdf
de Waal, A., Weaver, M., Day, T., & van der Heijden, B. (2019). Silo-busting: Overcoming the greatest threat to organizational performance. *Sustainability*, *11*(23), 6860. https://doi.org/10.3390/su11236860
Department of transport UK. (2017). *Cyber Security for Ships*. https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice
Det Norske Veritas. (2022, 27 June). *IACS unified requirements for cyber security mandatory from 1 January 2024*. DNV.com. https://www.dnv.com/news/iacs-unified-requirements-for-cyber-security-mandatory-from-1-january-2024-227429
Divine Caesar, L., Cahoon, S., Fei, J., & Sallah, C. A. (2021). Exploring the antecedents of high mobility among ship officers: empirical evidence from Australia. *Maritime Policy & Management*, *48*(1), 109-128. https://doi.org/10.1080/03088839.2020.1762012
DMA. (n.d.). *Cyber and Information Security - Strategy for the Maritime Sector*. https://dma.dk/Media/637709330853499994/Cyber%20and%20Information%20Security%20Strategy%20for%20the%20Maritime%20Sector.pdf
Drew, M. (2007). Information risk management and compliance—expect the unexpected. *BT Technology Journal*, *25*(1), 19-29. https://doi.org/10.1007/s10550-007-0004-x
Dworkin, S. L. (2012). Sample size policy for qualitative studies using in-depth interviews. *Arch Sex Behav*, *41*, 1319-1320. https://doi.org/10.1007/s10508-012-0016-6
Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93-125. https://doi.org/10.1111/rmir.12169
Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17*(5), 474-491. https://doi.org/10.1108/JRF-09-2016-0122
ENISA. (2011). *Analysis of cyber security aspects in the maritime sector - European Union Agency for Cybersecurity*. https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1
ENISA. (n.d.). *What is "Social Engineering"?* European Union Agency for Cybersecurity. https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering
Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security*, *2017*(2), 5-10. https://doi.org/10.1016/S1361-3723(17)30013-1
Gochhayat, J., Giri, V. N., & Suar, D. (2017). Influence of organizational culture on organizational effectiveness: The mediating role of organizational communication. *Global Business Review*, *18*(3), 691-702. https://doi.org/10.1177/0972150917692185
Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report*, *8*(4), 597-607. https://doi.org/10.46743/2160-3715/2003.1870
Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
Hayes, A. F., & Krippendorff, K. (2007). Answering the call for a standard reliability measure for coding data. *Communication methods and measures*, *1*(1), 77-89. https://doi.org/10.1080/19312450709336664
Holmemo, M. D.-Q., & Ingvaldsen, J. A. (2016). Bypassing the dinosaurs?–How middle managers become the missing link in lean implementation. *Total Quality Management & Business Excellence*, *27*(11-12), 1332-1345. https://doi.org/10.1080/14783363.2015.1075876

Hopcraft, R., & Martin, K. M. (2018). Effective maritime cybersecurity regulation–the case for a cyber code. *Journal of the Indian Ocean Region*, *14*(3), 354-366. https://doi.org/10.1080/19480881.2018.1519056
Hopkin, P. (2018). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Kogan Page Publishers.
Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660. https://doi.org/10.1111/j.1540-5915.2012.00361.x
IACS. (n.d.). *IACS adopts new requirements on cyber safety*. International Association of Classification Societies. https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/
Jarjoui, S., & Murimi, R. (2021). A framework for enterprise cybersecurity risk management. In *Advances in cybersecurity management* (pp. 139-161). Springer. https://doi.org/10.1007/978-3-030-71381-2_8
Johannessen, A., Christoffersen, L., & Tufte, P. A. (2016). *Introduksjon til samfunnsvitenskapelig metode* (fifth ed.). Abstrakt.
Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *J Adv Nurs*, *72*(12), 2954-2965. https://doi.org/10.1111/jan.13031
Kathuria, R., Joshi, M. P., & Porth, S. J. (2007). Organizational alignment and performance: past, present and future. *Management Decision*. https://doi.org/10.1108/00251740710745106
Kelman, H. C. (1958). Compliance, identification, and internalization three processes of attitude change. *Journal of conflict resolution*, *2*(1), 51-60. https://doi.org/10.117/002200275800200106
Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African journal of business management*, *5*(26), 10862. https://doi.org/10.5897/AJBM11.067
Kilpi, V., Solakivi, T., & Kiiski, T. (2021). Maritime sector at verge of change: learning and competence needs in Finnish maritime cluster. *WMU Journal of Maritime Affairs*, *20*, 63-79. https://doi.org/10.1007/s13437-021-00228-0
Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security. https://doi.org/10.14722/usec.2014.23007
Kosub, T. (2015). Components and challenges of integrated cyber risk management. *Zeitschrift für die gesamte Versicherungswissenschaft*, *104*, 615-634. https://doi.org/10.1007/s12297-015-0316-8
Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, *8*(6), 898. https://doi.org/10.3390/app8060898
Larsen, M. H., & Lund, M. S. (2021). Cyber risk perception in the maritime domain: a systematic literature review. *IEEE Access*, *9*, 144895-144905. https://doi.org/10.1109/ACCESS.2021.3122433
Leedy, P. D., & Ormrod, J. E. (2021). *Practical research: planning and design* (12th ed.). Pearson Education.
Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017
Linkov, I., Anklam, E., Collier, Z. A., DiMase, D., & Renn, O. (2014). Risk-based standards: integrating top–down and bottom–up approaches. *Environment Systems and Decisions*, *34*(1), 134-137. https://doi.org/10.1007/s10669-014-9488-3

Liu, L., Feng, Y., Hu, Q., & Huang, X. (2011). From transactional user to VIP: how organizational and cognitive factors affect ERP assimilation at individual level. *European Journal of Information Systems*, *20*(2), 186-200. https://doi.org/10.1057/ejis.2010.66

Luftman, J., Lyytinen, K., & Zvi, T. b. (2017). Enhancing the measurement of information technology (IT) business alignment and its influence on company performance. *Journal of Information Technology*, *32*(1), 26-46. https://doi.org/10.1057/jit.2015.23

Manfreda, A., & Štemberger, M. I. (2019). Establishing a partnership between top and IT managers: A necessity in an era of digital transformation. *Information Technology & People*, *32*(4), 948-972. https://doi.org/10.1108/ITP-01-2017-0001

Marotta, A., & McShane, M. (2018). Integrating a proactive technique into a holistic cyber risk management approach. *Risk Management and Insurance Review*, *21*(3), 435-452. https://doi.org/10.1111/rmir.12109

Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, *15*. https://doi.org/10.12716/1001.15.03.04

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International journal of qualitative methods*, *1*(2), 13-22. https://doi.org/10.1177/160940690200100202

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evid Based Nurs*, *18*(2), 34-35. https://doi.org/10.1136/eb-2015-102054

NSM. (2022). *Nasjonalt digitalt risikobilde*. Nasjonal Sikkerhetsmyndighet. https://nsm.no/getfile.php/1312007-1667980738/NSM/Filer/Dokumenter/Rapporter/NDIG2022_online.pdf

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, 60-68. https://doi.org/10.1109/STAST.2011.6059257

Oruc, A. (2022). Ethical considerations in maritime cybersecurity research. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, *16*. https://doi.org/10.12716/1001.16.02.14

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), 489-510. https://doi.org/10.1515/jhsem-2014-0035

Polkinghorne, D. E. (2005). Language and meaning: Data collection in qualitative research. *Journal of counseling psychology*, *52*(2), 137. https://doi.org/10.1037/0022-0167.52.2.137

Preston, D. S., & Karahanna, E. (2009). Antecedents of IS strategic alignment: a nomological network. *Information systems research*, *20*(2), 159-179. https://doi.org/10.1287/isre.1070.0159

Rezvani, Z. (2017). Who is a middle manager: A literature review. *extremes*, *1*, 44. https://doi.org/10.15226/2577-7815/1/2/00104

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *computers & security*, *56*, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

Singh, A. N., Picot, A., Kranz, J., Gupta, M., & Ojha, A. (2013). Information security management (ism) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management*, *14*, 225-239. https://doi.org/10.1007/s40171-013-0047-4

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Taylor, J. (2014). Organizational culture and the paradox of performance management. *Public performance & management Review*, *38*(1), 7-22. https://doi.org/10.2753/PMR1530-9576380101
Tessier, S., & Otley, D. (2012). A conceptual development of Simons' Levers of Control framework. *Management accounting research*, *23*(3), 171-185. https://doi.org/10.1016/j.mar.2012.04.003
Van Zeeland, I., Van den Broeck, W., Boonen, M., & Tintel, S. (2021). Effects of digital mediation and familiarity in online video interviews between peers. *Methodological Innovations*, *14*(3). https://doi.org/10.1177/20597991211060743
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004
Ward, J., & Peppard, J. (1996). Reconciling the IT/business relationship: a troubled marriage in need of guidance. *The journal of strategic information systems*, *5*(1), 37-65. https://doi.org/10.1016/S0963-8687(96)80022-9
Watkins, S. G. (2013). *An introduction to information security and ISO27001:2013 : a pocket guide* (Second edition. ed.). IT Governance Publishing.
Whitman, M. E., & Mattord, H. J. (2019). *Management of information security* (6th ed.). Cengage.
Yin, R. K. (2018). *Case study research and applications: design and methods* (6th ed.). SAGE.
Østby, G., Kowalski, S. J., & Katt, B. (2020). Towards a Maturity Improvement Process–Systemically Closing the Socio-Technical Gap. https://hdl.handle.net/11250/2737120

Appendices

Appendice 1: Interview guide [English]

Consent

Consent to record. You can ask for access, removal or changes of the material at any time.

Introduction

Introduction of ourselves

Background

Can you tell us about your educational background?

What is your job title/role? For how long have you been working in this position?

Have you worked at sea? If so, how many years experience do you have?

Can you take us through a typical workday?

- What are your work tasks?
- Which areas of responsibility do you have?

Cyber security

We will start with some general questions regarding cyber security.

What is your understanding of cyber security?

- How do you handle cybersecurity in your everday life?
- What kind of measures do you take yourself to limit cyber risks?

How do you perceive the work with cyber security?

- Oppfølgingspunkter: Meningsfullt, motivasjon, teknologi-fokusert eller menneskefokusert
- Sammenlignet med andre sikkerhetstiltak, for eksempel mtp. fysisk sikkerhet.

What would you say are the biggest focus points regarding cyber security within Kongsberg Maritime?

- Big focus on policies?

Risikostyring

Now, we would like to ask some questions regarding risk management, especially with cyber security and risks in mind.

Generally, what do you believe are the biggest cyber risks onboard ships?

- Navigation, communications

Can you say something about how you work with cyber risks within Kongsberg Maritime?

- Do you have many routines?
- Are there anyone that assure compliance with policies?
- Do you have a lot of trust?

How is your impression of other departments within Kongsberg Maritime, what is their perception of cyber security?

In your opinion, how do you think middle managers perceive cyber security?

- Does managers trust the security team and your evaluations?

Halvard mentioned you distinguish between awareness and training, how would you describe this relationship?

- Does people have an understanding of cyber security, or is it basic awareness?
- Is this something you work with? Do you train people for example?

How do you work to ensure that employees also focus on cyber security in their work?

What are your thoughts on cyber champions, is this something you are actively working with?

Do you know how risk assessments are carried out in the organization?

- Who decide the risk appetite?

How do you make sure that employees are aware of risks in their own work?

- How do you communicate risk to the employees?

If you discover a risk, how do you communicate that risk? And to who?

How do you work to build cyber culture within your organization?

Autonomous vessels

We would like talk a little bit about autonomous vessels

Do you have any knowledge of autonomous vessels?

The International Maritime Organization (IMO) has four levels of autonomy. Have you heard about these levels before?

- Level 1 has seafarers onboard to control the ship.
- Level 2 is controlled from another location but have seafarers on board.
- Level 3 is controlled from another location, with no seafarers on board.
- Level 4 is full autonomy; the operating systems takes its own decisions.

Which level do you believe the shipping industry is at today?

Which level do you believe is possible to achieve?

Do you have any thoughts on cyber security in autonomous vessels?

With cyber security in mind, do you think seafarers today has the competencies to work at a remote operating center?

Do you think there are new risks connected to a high level of autonomy? For example level 3?

Compared to your workday today, do you think it will change if remote operating center becomes a reality?

The number of seafarers are going down, but changes such as remote operating centers can slow this development. You have less travel, you can work "normal" hours and so on. What are your thoughts on this?

Elaborating questions (if time):

Can you tell us about a cyber incident you've experienced at work?

- How was it handled? Routines? Lessons learned?

How would you describe the development of maritime cyber security in recent years?

In your opinion, are cyber security seen as an important part of the organization?

How do you communicate cyber risks within the organization?

What kind of cyber security training does your employees receive?

What do you believe are the biggest challenges for good cyber security culture?

In your opinion, which factors can affect how you perceive cyber risk?

Now that operational technology and IT are becoming more integrated, would you say there are any changes in how the organization work with cyber security?

Appendice 2: Interview guide [Norwegian]

Samtykke

Samtykke til opptak. Du kan be om innsyn, sletting eller endringer av materialet på hvilket som helst tidspunkt.

Introduksjon

Introduksjon av oss selv.

Bakgrunn

Hvilken utdanningsbakgrunn har du?

Hva er stillingstittelen din? Og hvor lenge har du arbeidet i denne stillingen?

Hvis du har vært på sjøen, hvor mange års erfaring har du derfra?

Hvordan ser en typisk arbeidshverdag ut for deg?

- Hva er dine arbeidsoppgaver?
- Hvilke ansvarsområder har du?

Cybersikkerhet

Først noen generelle spørsmål knyttet til cybersikkerhet.

Hva er din forståelse av cybersikkerhet?

- Hvordan forholder du deg til dette i hverdagen?
- Hvilke tiltak utfører du selv i hverdagen for å begrense cyberrisikoer?

Hvordan oppfatter du selv arbeidet med cybersikkerhet?

- Oppfølgingspunkter: Meningsfullt, motivasjon, teknologi-fokusert eller menneskefokusert
- Sammenlignet med andre sikkerhetstiltak, for eksempel mtp. fysisk sikkerhet.

Hva vil du si er det største fokusområdet innenfor cyber sikkerhet i Kongsberg Maritime?

Risikostyring

I denne delen skal vi snakke litt om risikostyring. I hovedsak tenker vi på risikostyring i forbindelse med cybertrusler.

Generelt, hva tror du er den største risikoen på skip?

Med tanke på risiko og cybersikkerhet, hvordan ser en vanlig arbeidshverdag ut for deg?

- Preget av rutiner?
- Føler man seg kontrollert?
- Tillit fra ledelsen?

Hvordan jobber dere for at ansatte også fokuserer på cybersikkerhet i eget arbeid?

- Hvordan tror du ansatte opplever cybersikkerhets-arbeidet?

Har du noen tanker om hvordan mellomledere oppfatter arbeidet med cybersikkerhet?

Kjenner du til risikovurderingene som gjøres knyttet til eget arbeid?

Kjenner du til hvordan risikovurderinger gjennomføres?

- Blir det tatt risikovurderinger for organisasjonen som helhet, eller i hver enkelt avdeling?
- Hvor ofte blir disse vurderingene tatt?

Utarbeider dere rutiner ut ifra risikovurderingene, i så fall, hvilke rutiner har dere i din avdeling?

- Er rutinene tilpasset hver avdeling?

Hvem definerer akseptabelt risikonivå og ut ifra hvilke kriterier?

Hvem sørger for at de ansatte er klar over risikoer i egen arbeidshverdag?

- Nærmeste leder, noen høyere opp?

Hvordan blir du motivert til å følge rutiner for risikohåndtering?

- Oppfølgingspunkter: Motivasjon fra leder, motivasjon i dag

Hvordan arbeider dere for å bygge en cyberkultur i organisasjonen?

- Cyber champions

Autonome fartøy

Nå ønsker vi å prate litt om autonome fartøy.

Hvilken kjennskap har du til autonome fartøy?

International maritime organization (IMO) beskriver fire nivåer av autonomi:

Nivå 1: Skip med automatiserte prosesser og beslutningsstøtte	Det er sjøfarere ombord for å betjene og kontrollere systemer og funksjoner
Nivå 2: Fjernstyrt skip med sjøfarere om bord.	Skipet er kontrollert og betjent fra en annen lokasjon, men det er sjøfarere om bord.
Nivå 3: Fjernstyrt skip uten sjøfarere om bord.	Skipet er kontrollert fra en annen lokasjon, og det er ingen sjøfarere om bord.
Nivå 4: Fullstendig autonomt skip	Operasjonssystemet på skipet tar beslutninger og bestemmer handlinger selv.

Hvilket nivå mener du skipsfarten er på i dag, og hvilket nivå tror du er mulig å oppnå?

- Hva kreves for å oppnå dette nivået?

Har du noen tanker om cybersikkerhet rundt autonome fartøy?

Med tanke på cybersikkerhet, tror du sjøfarere i dag har kompetansen til å arbeide i et remote operating center?

Kan du se for deg noen nye risikoer ved høyt grad av autonomi *(for eksempel level 3)*?

Sammenlignet med arbeidshverdagen i dag, hvordan tror du arbeidshverdagen din vil endres dersom remote operating center blir en realitet?

Ifølge blant annet BIMCO er antall sjøfarere på vei nedover, og at tiltak som remote operating center kan bremse denne utviklingen fordi man har mindre reise, kan ha 'vanlige' arbeidstider og lignende.

Hva er dine tanker om dette?

- Oppfølgingspunkter: Motivasjon og kultur

Utdypende spørsmål (hvis vi får tid)**:**

Kan du fortelle oss om en cyberhendelse du har opplevd på jobb?

- Oppfølgingspunkter: Håndtering, rutiner, læring i etterkant

Hvordan vil du beskrive utviklingen av cybersikkerhet de senere årene?

- Er det noen utfordringer knyttet til dette?

Blir cybersikkerhet sett på som viktig i organisasjonen?

Hvordan kommuniseres cyberrisikoer i organisasjonen?

Hvilken trening/opplæring får de ansatte innenfor cybersikkerhet?

Kan du beskrive rutinene dere har for cybersikkerhetshendelser i dag?

Mange tenker brannmurer og kryptering når de hører ordet cybersikkerhet, men vi ser at cyberangrep blir mer og mer sofistikerte. For eksempel såkalt social engineering, det er at man utnytter menneskelige feil for å få tilgang til systemer. Et eksempel er at angripere utgir seg fra å være en ansatt på IT som skal hjelpe deg med datamaskinen din, trenger bare passordet osv...

Hvordan blir slike (*social engineering og lignende*) cyberrisikoer kommunisert i organisasjonen?

Hvordan tror du kulturen for cybersikkerhet er i organisasjonen?

- Hvorfor tror du det?

Hva tror du er den største utfordringen for god cyberkultur?

Hva tror du kan påvirke oppfattelsen av cyberrisikoer?

Kjenner du til forskjellen på operasjonell teknologi og informasjonsteknologi? Såkalt OT og IT?

Kort forklart er teknologi knyttet til drift av utstyr, for eksempel navigasjonssystemer og styring av propeller. *IT er systemer og nettverk, data og så videre.*

Har du noen tanker om endring av risiko når operasjonell teknologi og informasjonsteknologi i større grad integreres?

- Hvordan tror du arbeidshverdagen din vil endres som følge av dette?

Appendice 3: Information letter and consent form [English]

Gjøvik / 24.03.23

Information letter

We are two students taking a Masters in Industrial innovation and digital security at NTNU in Gjøvik. We are writing our master with Kongsberg Maritime as case-organization. The project title is:

«New risks of autonomous vessels: ensuring cyber security along with increased autonomy in the maritime industry".

Purpose
The purpose of the master's thesis is to investigate how maritime organizations can facilitate good risk management of cyber risks, especially with regard to autonomous ships and land-based operations centers.

Participation
You are being asked to participate because you fall within our target group, defined as employees in the maritime industry between the ages of 20 and 70. If you choose to participate, we would like to have an interview with recording, where notes will also be taken during the interview. The interview will last approx. one hour.

Voluntary participation
Participation is voluntary. You can at any time be able to withdraw consent, request access, corrections or deletion, by verbal or written message without specifying a reason.

Privacy: collection, storage, processing and use of your information.
No sensitive personal data (see Articles 9 and 10 of the General Data Protection Regulation) will be collected. Personal information about you will only be used for the purposes described in this information letter. We treat the information confidentially and in accordance with the privacy regulations.

Personal data that is processed:

- Name (also with signature/consent)
- Address or telephone number
- E-mail address
- Audio recording of people
- Background information that will be able to identify a person
    - Age, education, previous work experience
- Other information that will be able to identify a person
    - Job title

We process personal data in order to get in touch with informants and understand the background for statements. Recording of interviews is done to make the work process more orderly, and to ensure correct citation.

Informants will not be able to be directly or indirectly identified in the thesis or other publications. Personal data will be stored separately from other data. At the end of the project, the data will be anonymized through rewriting of personal data or deletion.

Lawfulness of processing
Processing of personal data takes place on the basis of consent, cf. the General Data Protection Regulation art. 6 no. 1 letter a.

Institution responsible for processing
Norwegian University of Science and Technology / Faculty of Economics and Management (OK) / Department of Industrial Economics and Technology Management.

Processing responsibility will not be shared with other institutions.

Rights
We process information about you based on your consent. As long as you can be identified in the data material, you have the right to:

- View which personal data is registered on you, and be given a copy of the data,
- To have personal data about you corrected, and
- To send a complaint to the Norwegian Data Protection Authority about the processing of your personal data

Responsible for the project (supervisor)
Oda Ellingsen, oda.ellingsen@ntnu.no, tlf: 90159393.

If you have questions about the project, or wish to make use of your rights, contact Embla Jenssen, Sindre Johansen or our supervisor Oda Ellingsen.

Before the interview, we ask you to consent to participation.

Kind regards,

Embla Jenssen
emblaj@ntnu.no

Sindre Johansen
sindjo@ntnu.no

Declaration of consent

I have received and understood the information about the project, and have been given the opportunity to ask questions. I agree to:

Interview and recording of interview.

I consented to my data being processed until the end of the project.

_____
Place and date

_____
Full name

Appendice 5: Information letter and consent form [Norwegian]

Gjøvik / 24.03.23

Informasjonsskriv

Vi er to studenter på master i industriell innovasjon og digital sikkerhet, og skriver masteroppgave med prosjekttittel:
«New risks of autonomous vessels: ensuring cyber security along with increased autonomy in the maritime industry»

Formål

Formålet med masteroppgaven er å undersøke hvordan maritime organisasjoner kan tilrettelegge for god risikohåndtering av cyberrisikoer, spesielt med tanke på autonome skip og landbaserte operasjonssentre.

Deltakelse

Du blir spurt om å delta fordi du faller innenfor vår målgruppe, definert som ansatt i den maritime industrien i alderen 20 – 70 år. Dersom du velger å delta ønsker vi å ha et intervju med opptak, hvor det også vil bli tatt notater underveis i intervjuet. Intervjuet vil vare ca. en time.

Frivillig deltakelse

Det er frivillig å delta. Du kan når som helst kunne trekke samtykke, be om innsyn, rettelser eller sletting, ved muntlig eller skriftlig beskjed uten å oppgi grunn.

Personvern: innsamling, oppbevaring, behandling og bruk av dine opplysninger.

Ingen sensitive personopplysninger (jf. Personvernforordningens artikkel 9 og 10) vil bli innsamlet. Personlige opplysninger om deg vil kun benyttes til formålene beskrevet i dette informasjonsskrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

Personopplysninger som blir behandlet:

- Navn (også ved signatur/samtykke)
- Adresse eller telefonnummer
- E-postadresse
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person
    - Alder, utdanning, tidligere arbeidserfaring
- Andre opplysninger som vil kunne identifisere en person
    - Arbeidstittel

Vi behandler personopplysninger for å komme i kontakt med informanter og forstå bakgrunnen for uttalelser. Opptak av intervjuer blir gjort for å gjøre arbeidsprosessen ryddigere, og for å sikre korrekt sitering.

Informanter vil ikke kunne direkte eller indirekte identifiseres i oppgaven eller øvrige publikasjoner. Personopplysninger vil oppbevares atskilt fra øvrige data. Ved prosjektslutt vil dataene anonymiseres gjennom omskrivning av personopplysninger eller sletting.

Behandlingens grunnlag

Behandling av personopplysninger foregår på grunnlag av samtykke, jf. Personvernforordningen art. 6 nr. 1 bokstav a.

Behandlingsansvarlig institusjon

Norges teknisk-naturvitenskapelige universitet / Fakultet for økonomi (ØK) / Institutt for industriell økonomi og teknologiledelse.

Behandlingsansvaret vil ikke deles med andre institusjoner.

Rettigheter

Vi behandler opplysninger om deg basert på ditt samtykke. Så lenge du kan identifiseres i datamaterialet har du rett til:

- Innsyn i hvilke personopplysninger som er registrert på deg, og få utlevert en kopi av opplysninger,
- Å få rettet personopplysninger om deg, og
- Å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Prosjektansvarlig (veileder)

Oda Ellingsen, oda.ellingsen@ntnu.no, tlf: 90159393.

Hvis du har spørsmål til undersøkelsen, eller ønsker å benytte deg av dine rettigheter, ta kontakt med Embla Jenssen, Sindre Johansen eller vår veileder Oda Ellingsen.

Før intervjuet ber vi deg om å samtykke deltagelsen ved å …

Med vennlig hilsen

Embla Jenssen
emblaj@ntnu.no

Sindre Johansen
sindjo@ntnu.no

Samtykkeerklæring

Jeg har mottatt og forstått informasjonen om undersøkelsen, og har fått anledning til å stille spørsmål. Jeg samtykker til:

Intervju og opptak av intervju.

Jeg samtykket til at mine opplysninger kan behandles frem til prosjektslutt.

_____
Sted og dato

_____
Fullt navn

Appendice 6: Data handling plan [Only Norwegian]

New risks of autonomous vessels: ensuring cyber security along with increased autonomy in the maritime industry

Master thesis: Research on cyber security on autonomous vessels.

Fagområder

Landbruks- og fiskerifag, Samfunnsvitenskap, Teknologi

Forskningsansvarlig institusjon

Norges teknisk-naturvitenskapelige universitet / Fakultet for økonomi (ØK) / Institutt for industriell økonomi og teknologiledelse

Prosjektvarighet

01.01.2023 — 15.05.2023

Formål

Forske på cybersikkerhet rundt autonome fartøy hos Kongsberg Gruppen. Forskningsspørsmål: "How to manage new cyber risks of autonomous vessels in the maritime industry?". Belyses gjennom observasjon og intervjuer.

Nytteverdi

Kongsberg Gruppen. Relevante faggrupper ved NTNU og tilsvarende fagmiljøer. Fagområder: informasjonssikkerhet og maritim.

Etiske retningslinjer

- Generelle forskningsetiske retningslinjer
- Naturvitenskap og teknologi
- Samfunnsvitenskap, humaniora, juss og teologi

Intervju og observasjon

Beskrivelse

Intervju med informanter og observasjon av Kongsberg Maritime.

Datatype

Lyd, Tekst, Datasett

Språk

Engelsk, Norsk

Nøkkelord

autonomi, cybersecurity, maritim, informasjonssikkerhet, vessels, ships, unmanned vessels

Data om personer

Ja

Er det noen andre grunner til at dataene dine trenger ekstra beskyttelse?

Nei

Kategorier av personopplysninger

Alminnelige

Utvalgets størrelse

10

Innsamlingsperiode

01.01.2023 — 15.05.2023

Innsamlingsenheter

- 2. NTNU Microsoft Teams
- 4. Ekstern lydopptaker/diktafon

Datakvalitet

Transkribering og observasjon.

Metode

Intervju, Observasjon, Opptak, Transkripsjon

Størrelse

100000 MB

Format

doc, pdf, lydfiler, xls

Programvare

Microsoft Word, NVIVO, Microsoft Teams, Lydopptaker

Lagring

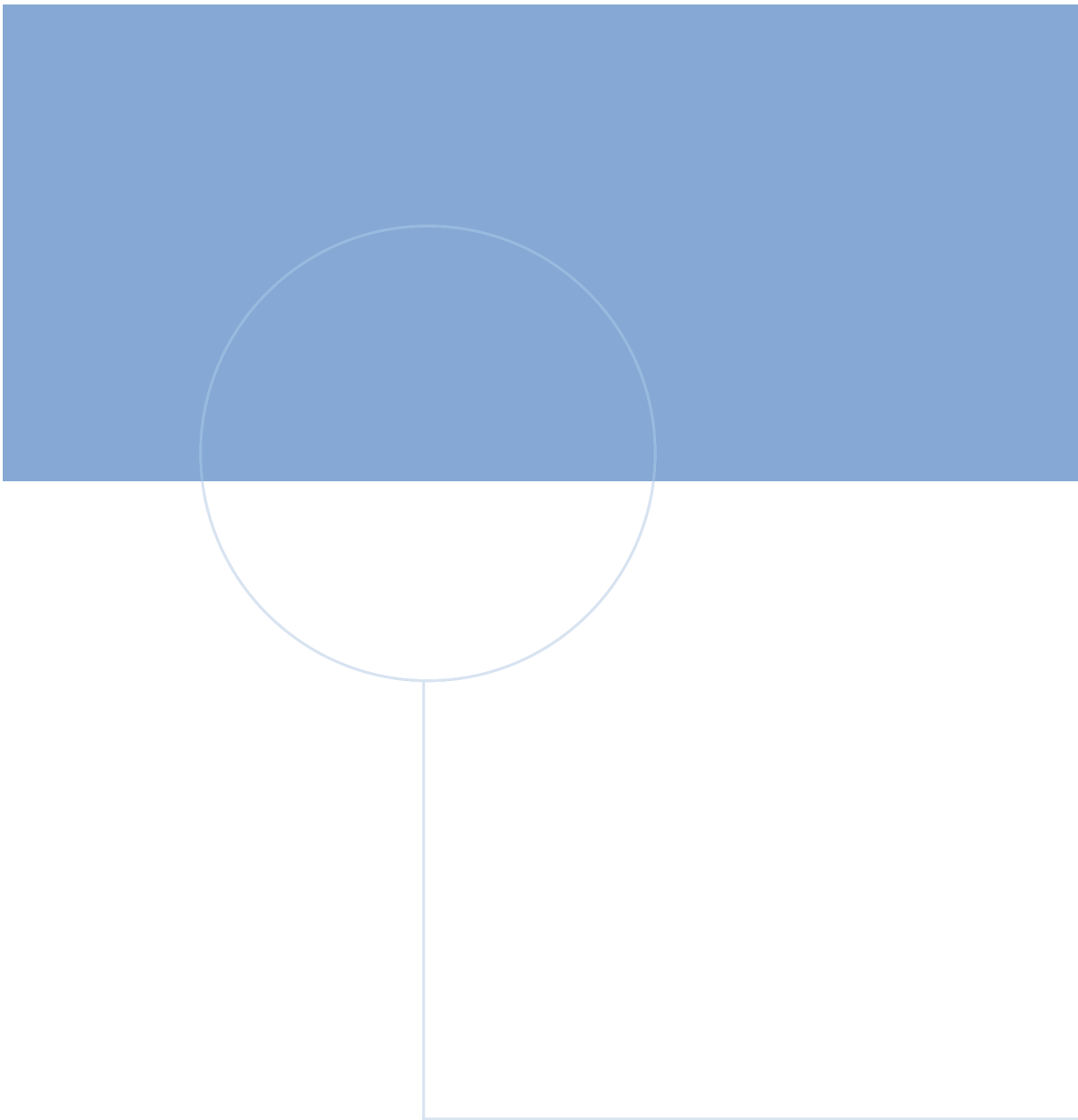
- 05. NTNU Office 365 (SharePoint, Teams, Onedrive)
- 14. Annen lagringsløsning

Overføring

- 2. Office 365 (SharePoint, Teams, Onedrive)

Arkivering

Nei



NTNU

Norwegian University of
Science and Technology