University of South-Eastern Norway

Cyber security Risk perception and Mitigation Strategies within the Maritime Shipping Industry

Candidate name: Valerie- Peggy Immy Korsvik

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

MASTER OF SCIENCE IN MARITIME MANAGEMENT

SUPERVISOR: ASSOCIATE PROFESSOR ZIAUL HAQUE MUNIM

November 2023

Abstract

The severity of cyber security requires global attention and consciousness given its ramifications to both companies and the global economy. Each year predictions indicate an exponential intensification in number of daily cyber-attacks and economic losses associated to cybersecurity.

The shipping industry and the global economy are closely interlinked to each other. The maritime shipping is responsible for around 95% seaborne trade making it a life blood in world trade and the global economy. With such economic muscle the sector is increasingly adapting new and better operation technologies within their infrastructure, putting them on the front squad for malicious ransom activities under which cybersecurity attacks are embedded. The consequences of such malicious activities can be severe beyond property and economic interests, extending to human lives, environment, and the economy entirely.

The seriousness of this matter poses ongoing challenges to Maritime shipping stakeholders making it a hot topic attracting continuous scholarly attention. There is a need to further address issues of awareness on cybersecurity and the mitigation procedures. Therefore, Exploration of risk perceptions and mitigation strategies from the maritime shipping perspective is a relevant study.

Two main research questions guided the study. The perception of cyber risk amongst seafarers and managers; What Mitigation strategies are applied before, during and after cyberthreats. The study used a web-survey with Likert type questionnaire, distribution was purposively through LinkedIn and snowball recruitment. Out of 30 respondents, 22 usable responses form this study findings. The participants had vast work experiences and backgrounds ranging from ship owners, Maritime insurance, seafarers, Academics, and others from different managerial positions.

Regarding cyberthreat perception, we find a fair understanding of its seriousness in participants. However, threat identification is still a challenge, the company procedures seem unclear to understand and recite. Regarding mitigation strategies, there seem to be less focus on strategies undertaken during and after the threat, but more on the preventive ones. This can be unfortunate and thus require more direction.

Key words – Cybersecurity- Risk, Cyber threats, Risk assessment, Mitigate, shipping industry, Human risk perception, Risk mitigation, Web- survey, Risk analysis.

Acknowledgement

My sincere thanks to my supervisor Assoc. prof. Ziaul Haque Munim, this piece would never be here right now if it was not because of your encouragement and valuable advice. Thank you so much being patient with me until the end.

Furthermore, to you my husband Axel A. Korsvik and my favourite son Josh Larry Gabula Korsvik, you guys mean the world to me. Thanks for the great support all the way, and I ask God, the one who looks after us to continue blessing us with love and care.

To my two sisters Alexis and Jannat, my Nieces, Nephews, Aunties, and cousins thanks for bearing with my absence on some occasions. My in laws the entire Korsvik- I am so blessed to have your support always.

To my friends and colleagues who paved the way for data collection in the Maritime shipping, my employer that offered flexibility thank you all. Thanks to unknown survey participants. Thanks to the almighty God that has seen me through to this day of submission.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ACRONYMS

AIS	Automatic Identification System
AR	Augmented Reality
AI	Artificial Intelligence
ABS	American Bureau of Standard
BIMCO	Baltic International Maritime Council
CI	Critical Infrastructure
CS	Cyber-security
CIA	Confidentiality Integrity Availability
CST&R	Cyber-security Threats & Risks
DNV	Den Norske veritas
DOC	Documentation of Compliance
DAI	Defense Action Intention
ECDIS	Electronic Chart Display & Inf. System
GNSS	Global Nav. Satellite System
ISPS	Intern.
ISPS	International ship and Port security
IMO	International Maritime Organization
IoT	Internet of Things
ISM	International Safety management Code
ICT	Information and Comm. Tech
IT	Information Technology
MITM	Man in The Middle
MASS	Maritime Automated Surface Ships
MCS	Maritime Cyber Security
NIST	National Inst. Of Science and Tech.
OT	Operational Technology
SME	Subject Matter Experts
VLANS	Vert. Local Area Networks
UNCTAD	United Nations Conference on Trade

CHAPTER ONE: INTRODUCTION

1.0 Chapter Overview

The maritime sector is a powerful and thriving industry considered a key driver of economic growth. The United Nations Conference on Trade and Development (UNCTAD) and International Chamber of Shipping (ICS) estimate 90% of the global trade volume being linked to maritime shipping industry, as well as annual freight rates of more than USD 380 billion (ICS, 2023; UNCTAD, 2022). The industry is integral to an international supply chain, a wide supply chain that stretches from sea voyage to port infrastructure, and inbound and outbound activities, making it a complex ecosystem with various stakeholders (Meland et al., 2021; Munim & Schramm, 2018; Stopford, 2008; Townsend, 2022; UNCTAD, 2020b). In such a context, the industry acts as a bedrock as it links together multiple parties in the global supply chain, stimulating economic growth, job creation and general wealthy and well-being of nations around the world. Therefore, what impacts the maritime, impacts the world as well. In this case, maritime cybersecurity is a global concern.

1.1 Research background

The ships are no longer those physical objects of the old era, whereby once the ship left the port, it was on its own, and any potential risk was limited to either human error or technical and mechanical failures, making any threat locally limited. Therefore cyber risks in maritime will have a huge damage globally (OECD, 2022; Townsend, 2022).The new technology considered to be reliable and efficient facilitates various communications between the ship and shore that has increased its adaptability, yet it must be mastered well by all users. The Automatic identification systems (AIS), Global Navigation Satellite Systems (GNSS), Electronic Chart Display and Information systems (ECDIS) are modern technologies on physical ships contributing to safe navigation, and because of their efficiency and reliability the future in maritime is predicted crewless. However, the proliferation of these technologies does not come trouble free, because they make ships prone to cyber security risks.

Cyber security in the maritime has a huge impact on the safety of crew, vessel, cargo, and ports. The Maritime sector is a leading source of employment in many countries, both directly and indirectly hence a bread winner to millions of households, as well as a future for continuous innovation (OECD, 2021), which makes discussions in regards to safety in broad an epitome for maritime stakeholders. Cybersecurity in shipping is concerned with protection of information technology (IT) systems, on board the ships 'hardware, sensors and data leakage

from/to unauthorised access, manipulation, and disruption. Cyber security plans and policies cover various risk types such as information integrity, system, and hardware availability both in shipping company´s offices and onboard the ship (BIMCO, et al., 2017; BIMCO, 2019; IMO, 2017b; Maritime safety committe, 2017). The International Maritime authority (IMO) identifies systems onboard the ship that are considered vulnerable, as baked in sector definition.

According to IMO (2017, p1) cyber security risk is defined, "a measure of the extent to which an asset, system, application, or connected infrastructure could be threatened by a potential circumstance or event which may result in shipping related operational, safety or security failures because of information or systems being corrupted lost or compromised" (IMO, 2017b). The International safety Management code (ISM) and the international ship and port facility security code (ISPS) have escalated to ensure safety in a risk management perspective (IMO, 2017b). The, need to raise CS awareness and safety assurance in shipping lies to the responsibility of various stakeholders as stipulated in IMOs annex p.1 (2017).

> Recognizing that administrations, classification societies, ship owners, and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities" (IMO, 2017b; Maritime safety committe, 2017).

The company procedure and guidelines should be in line with the safe management system context (SMS) (BIMCO, et al., 2017, p. 2), found in (ISM Code)[1] and ISPS Code[2] not later than the first annual verification of the companies' documentation of compliance (DOC) after January 1. 2021. The company is thus bearing an obligation of integrating cybersecurity as a company culture. The guidelines stipulate the need for all levels in the company to bear bare responsibility for CS, ranging from senior management ashore to onboard personnel, as an inherent part of the safety and security culture necessary for safe and efficient operation of the ship (BIMCO, et al., 2017).

The resilience of future companies and organisations is dependent on both internal and external stakeholders possessing a broad knowledge on implementation of emerging technologies (WEF, 2023). Cybersecurity is an issue high on many company's` agenda (BIMCO, 2019; DNV, 2022; Garry, 2023; GCE, 2023; IMO, 2022; OECD, 2022; WEF, 2023).

[1] https://www.imo.org/en/ourwork/humanelement/pages/ISMCode.aspx- The International safety management (ISM) Code main purpose is to provide an international standard for the safe management and operation of ships and for pollution prevention.

[2] International ship and port facility security code

The cost of vulnerability is being estimated, and it varies widely based on data and method (McNicholas, 2016). Several sources estimate the range from $300 billion each year as a lowest figure, to over $2 trillion a year or even more. The number is even projected to over $ 10.5[3] trillion by (Freeze, 2020; Marr, n.d.; McNicholas, 2016, pp. 281–287; WEF, 2023). With such huge estimate and severe consequences in terms of human causalities, economic and environmental cyber security is huge maritime concern as well as global.

Cyber-security is a topic mostly sought after, and a top agenda in several corporate conferences. For example, the World`s top knowledge network - World Economic Forum (WEF) in Davos January 18th 2023, theme: Global CS outlook 2023, and regional business cluster conference, 14th February 23 (GCE, 2023; WEF, 2023). The focus is cybersecurity to corporations and organisations, exacerbated by implementation of emerging technologies.

Maritime cyber security attacks (MCS- attacks) have been witnessed since 2010`s and they change forms and behavior. Recent updates include among others: 1) The 2023 ransomware that hit the servers of DNV- one of the world's leading classification societies and a recognised advisor for the maritime industry- according to Norwegian press (DN,2023, p17-17). The attack forced them to immediately shut down the server (Garry, 2023; Seatrade, 2023) affecting customers that depend on ship management (over 70 customers that operate more 1000 vessels). 2) The French container shipping company CMA CGM, after having been hit in 2020, (Cichen, 2020; CMACGM, 2020; Park et al., 2023a), has been retargeted again in 2021 (Shippingwatch, 2021). The ransomware in 2020, led to inaccessibility to company`s website and applications affecting several customers, similarly in 2021. 3) The high level international organisations (for example IMO and NATO) were attacked (Kovacs, 2020; Kuhn, Bicakci, et al., 2021), affecting IT systems including public website and their intranet systems. 4) Other large companies for example Maersk line, BW group, COSCO, and (Cichen, 2020; Shen, 2018; Wei Zhe, 2017) have fallen prey to data breaches and attacks recently.

Accidents that have happened due to failure of addressing cyberattacks have witnessed enormous consequences (Ben Farah et al., 2022; Meland et al., 2021). Affecting ports, supply chains, and loss of, reputation, asset loss, economic damages, environmental related to name but a few. For example, in 2017, the so called Not Petya- Maersk line, is said to have costed about $300 million in lost productivity (Greenberg, 2018; Park et al., 2023b), whereas the

[3] Press conference: Global cybersecurity outlook 2023 at the World Economic Forum at Davos January 18 2023 https://www.weforum.org/events/world-economic-forum-annual-meeting-2023/sessions/press-conference-global-cybersecurity-outlook-2023

COSCO terminal at the port of long beach in 2018, the IMO, CMA CGM, DNVGL in 2023 have suffered with networks broken down, affecting customers and thus their reputation.

In relation to the above concerns, the world`s major shipping organisations- together with The Baltic and international maritime council (BIMCO), have led high level discussions, resulting to the co-authoring and publication of the first ever "industry guidelines on cybersecurity on board ships"(BIMCO, 2019; BIMCO, et al., 2017; Maritime safety committe, 2017). This work gave a basis to the first IMO- Guidelines on maritime cyber risk management-- IMO doc. MSC- FAL .428 /Circ.3, and later to the maritime safety committee resolution- MSC.428 (98). IMO currently require ship owners and managers to assess cyber risk and implement relevant measures across all functions of their safety management systems (DNV, 2023) . It is a cumbersome process which leaves much of the interpretation to the company responsible, DNV preprepared recommended steps to easy the implementation of these obligations for stakeholders[4]

The sprang to new technologies in the maritime is believed to have been accelerated due to covid 19 pandemic. With its mandatory safety instructions of 1 metre distance and working from home via internet, the Maritime industry has had to play catch up (UNCTAD, 2020a, p. 49). The so called - playing a catch-up, meant that Maritime industry has had line up to the pace of other sectors. Believed to have adopted digitalisation and technology ex-ante (Rüßmann et al., 2015). The industry got more dependent to internet than ever, leading to adoption of new technologies (UNCTAD, 2020, 2023). The technology, they are constantly connected, automated and integrated include (Kavallieratos et al., 2020; Munim et al., 2020; Tusher et al., 2022a), often using IOT, block chain, bigdata, artificial intelligence (AI) among others to improve efficiency sustainability and resilience.

However, some of the systems and computers on ships often use complicated and old systems believed to potentially create blind spots. Other areas of shipping such as data and document sharing make use of blockchain technology. Additionally, ports are improving their openness, security infrastructure and management – using smart sensors and the IoT, along with terminal automation, port community systems, and traffic management systems. The global smart ports market for example is forecasted to increase from $ 1.9 billion to $ 5.7 billion

[4] https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/ism-guidance.html
DNV published recommended steps on how ship owners and managers can go about fulfilling the requirement of IMO and ISM, which effective from January 2021 became an obligation to all. The ISM supported by IMO resolution.

between 2022-2027 according to Clarkson (*2022: Shipping's Half Year Report | Clarksons*, 2023).

There is an increasing concern that stakeholders in the maritime industry are likely to be unaware of the criticality of CS(*CMA*, 2022). They are only possessing top of ice information yet; the iceberg is hidden. Scholars are concerned of the real risk of cybersecurity and that the subject, requires constant scholarly attention. Thus is already attracting a growing research (Karim, 2022; Kavallieratos et al., 2020), to find out how different stakeholders are coping with the challenges. Indeed, this acceleration is happening in the maritime sector and CS became a natural part of safety regulations, hence the integration of new clauses too (BIMCO, 2019).

1.2 Research Problem

Literature on CS in the maritime is limited compared to the growing insecurity and increasing daily attacks (Park et al., 2023a). Many organizations may lack appropriate information and knowledge due to insufficient or undisclosed incidents, knowledge on the risk and procedures to follow (Alshahrani et al., 2022; Park et al., 2023c; Ungkap & Daengsi, 2022a). The strategies employed to mitigate these problems are complex and dependent on a variety of aspects (Cheung et al., 2021; Larsen & Lund, 2021; Park et al., 2023a). Recent studies are still calling for more empirical studies (Ashraf et al., 2022; Cheung et al., 2021; Larsen & Lund, 2021; Park et al., 2019a, 2023c; Tusher et al., 2022a) to throw more light on the complexity. For example, after having proposed decision framework for assessing CS risks in autonomous shipping, they suggest an on-going update in various sectors. Maritime is naturally part of logistics. To this end, have recent studies made three categories to break down the complexity regarding mitigation strategies – as Real time recovery, Aftermath and precautionary (Cheung et al., 2021, pp. 4–5). Maritime is inseparable from supply chain and logistics, thus can be interesting to apply similar contexts. More studies specify a need to evaluate mitigation strategies for the list of risk they came up with, where Malware, Phishing and human factors are turbulent CS risks (Larsen & Lund, 2021; Park et al., 2023a)

To supplement these works above, this study contributes on the continuously growing knowledge on CS, seen from the seafarer's avenue, the managers and subject matter experts (SMEs) in the maritime shipping through questions below.

1.3 Research Questions(s)

Q1 How is Cyber security -Risk (CSR) perceived among seafarers and managers in the Maritime?

Qn2: What measures are taken to mitigate cyber security -risks?

This study aims at providing the reader insights on cyber security risks, threats, and the mitigation practices - seen from the maritime shipping perspective. Through collection of practices, this paper lines back other scholars to form a small contribution to this tantalizing problem, and even those outside maritime will find it useful. It may not be a pre-requisite for managers and seafarers or any other operators to be excellent IT experts, however a minimum is expected and is a necessity in today's operations- as a precaution against these ever-eroding risks.

1.4 Thesis Outline

The rest of this study is divided into six sections as follows: The second section presents the literature review about cybersecurity. The third section describes the methodology to be used. Section four is the findings generated, while five is the discussion. The paper comes to an end with the sixth section that bears the conclusion.

CHAPTER TWO: LITERATURE REVIEW

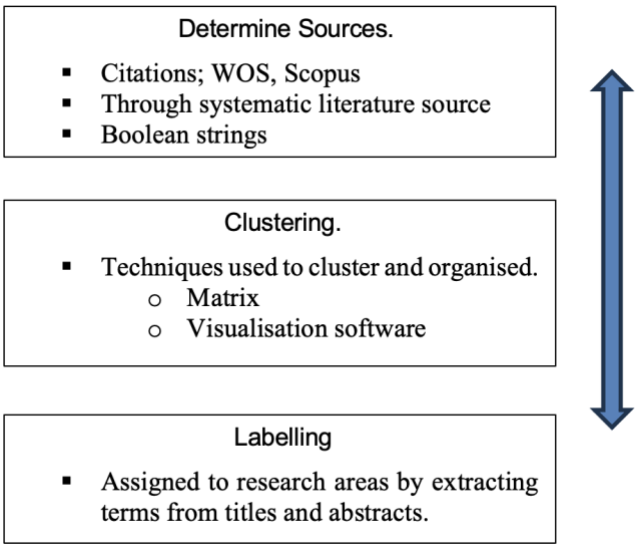
2.0 Chapter Overview

The chapter presents existing literature related to the study. Section 2.1 shows how the literature was found, 2.2 is a review of definition and conceptualisation of (CS). Section 2.3 presents a review of cybersecurity challenges and risks, while 2.4 the mitigation strategies. In section 2.5 a combine the concepts of CS, the mitigation strategies, categories, and measures to form a conceptual framework.

2.1 Method for finding and selecting literature**.**

To identify the relevant academic literature a bibliometric analysis was undertaken. Bibliometric analysis is commonly used in the maritime field for example (Munim et al., 2020). It provides several descriptive of authors, journals, based on citation and keywords, in addition to supporting the research clusters and providing insights into current research interests and trend. A three- step system illustrated below was followed based on a methodology for classification of publications and journals (Waltman & van Eck, 2012). The first was to determine sources for publications and journals and their relatedness. Then clustering and organising them into research areas and lastly labelling them. It is an iterative process of constant reading back and forth thereby enabling interlinkage in literature review.

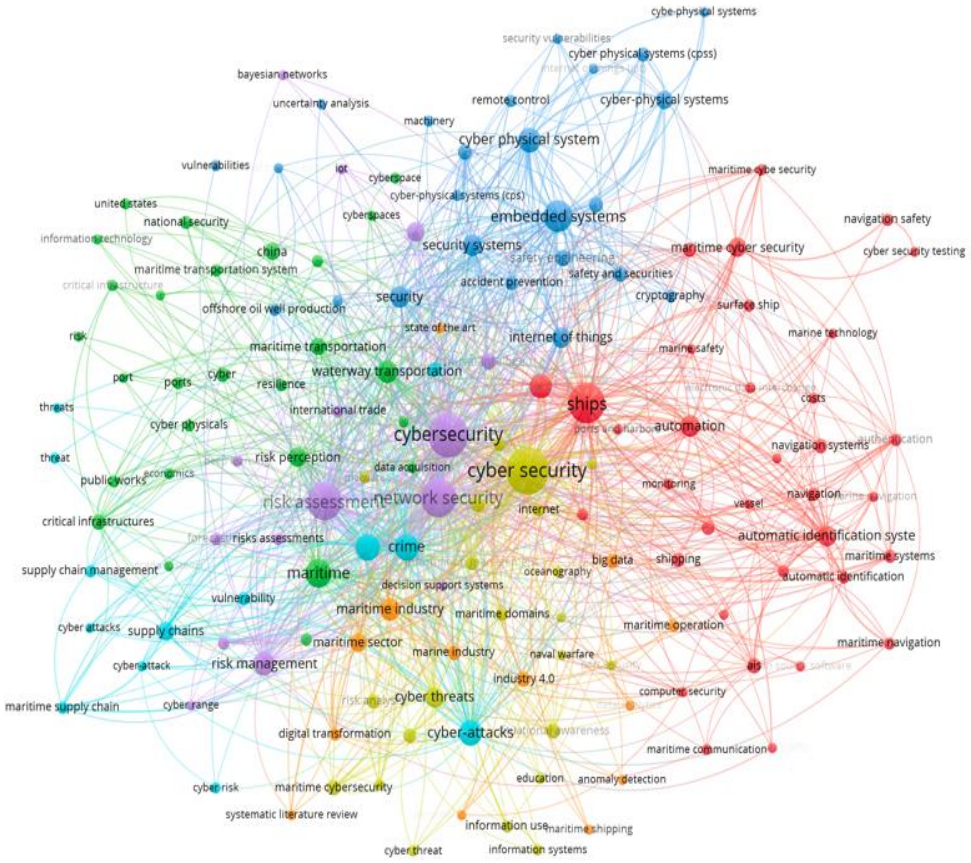
Figure 1: Three-step construction methodology



Source: own construct

Before writing the literature, a three-step methodology above illustrates the process in a three- way matrix. Determination of sources is a point where data collection through a systematic literature search start captured in a matrix – A-5 start in which bibliometric citation analysis is gathered in practice. The Boolean search strings were created with search terms; Cybersecurity, Cyber-security risks, Cybercrime, Cyberthreat, Threat mitigation, Perception, Cyber-resilience, Maritime, shipping, maritime cybersecurity among others as illustrated. The SCOPUS data base was used for all the English documents related to cybersecurity. To narrow down the search, various key words combinations are tried as search queries. The first search query is "(cybersecurity OR shipping (cyber AND security)) AND (Maritime OR Shipping)). This yielded four hundred (400), but after sorting out to closer preferences, one hundred thirty-nine (n= 139) are left for review. A visualisation of bibliometric mapping in Figure 2 based on Vos-viewer software (Eck & Waltman, 2009) was adopted. For interpretation, the colours illustrate the research areas and categories in line with research questions and search query. The figure tells that cybersecurity is seen in various perspectives within maritime and the attack ecosystem is complex. Ranges from ships, automations, navigations but the literature focus more on the shipping hence a bigger red dot as well as other big dotted areas.

Figure 2: Mapping bibliometric review



Source: own construct – based on (Eck & Waltman, 2009)

2.2 Labelling Reviewed literature

The fine tuning of search query "(cybersecurity OR (cyber AND security)) AND (Maritime OR Shipping)), gave over 300 articles - from disciplines such as computer science, engineering, management education, social sciences, decision science, Business management and accounting, energy among others. More publication is observed in the latest years especially from 2015 to 2023. More search re-refining resulted in n= 139 of which 90 were published as journal papers, while the rest were conferences.

2.3 Cybersecurity Perception

It is evident that information and communication technology (ICT) is ever evolving. The connectivity between Operational Technology (OT) and Information Technology (IT) is both the future and current driver of maritime operations (Afenyo & Caesar, 2023; Androjna & Perkovič, 2021; Ashraf et al., 2022; Barber et al., 2022; Cheung et al., 2021; Kanwal et al., 2022; Kechagias et al., 2022; Larsen & Lund, 2021; Meland et al., 2021; Park et al., 2019a; Tusher et al., 2022a). However, the integration is perceived vulnerable spot for cyber threats and risks on to critical infrastructures (CI) (Afenyo & Caesar, 2023; Kechagias et al., 2022), which despite some criticisms (Kanwal et al., 2022; Karim, 2022), has (IMO) together with other stakeholders and major classification societies have undertaken serious initiatives since 2017. The ISM code and ISPC requires all maritime stakeholders to document the integration of CS culture in own business operations (BIMCO, 2019; BIMCO, et al., 2017; DNV, 2023; Maritime safety committee, 2017; Meland et al., 2022). Implementation of CS culture requires knowledge capital and a clear international legal framework to enable a general mapping of maritime cyber security (MCS) to start with (Karim, 2022).

In their study that presented a nine dimensions framework of cyber risk perception (Larsen & Lund, 2021) to illustrate the complexity risk perception in the lenses of psychometric paradigm and cognitive biases. The perception of cybersecurity is beyond technical stand alone and use of such recognised psychological models form the understand of human perception as well as guiding in the development of mitigation tools. The psychometric is represented by nine dimensions (p.1488) to understand human risk perception. It is of great importance that leaders and managers are equipped against wrong security perceptions as they can be heavily detrimental(Kuhn, Bicakci, et al., 2021). Mistakes can be undermined or escalated as a result.

The ecosystem of cyber security perception thus starts from knowing what CS is, what types as discussed below.

2.3.1 Review of Cyber security.

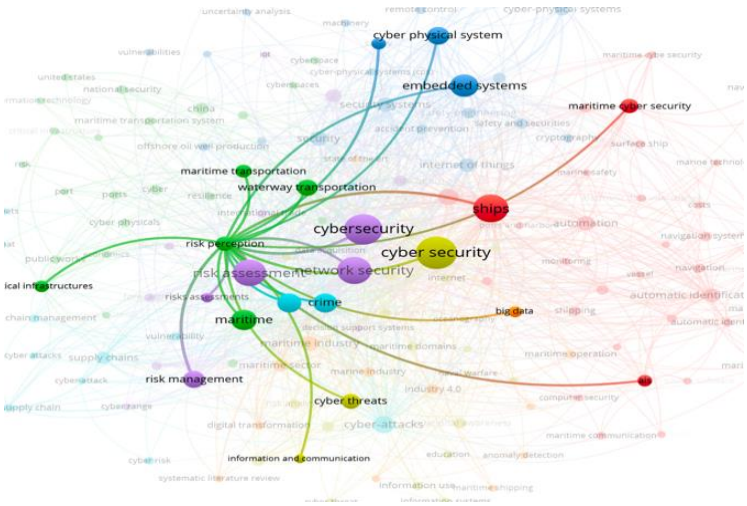
The is a broad review of cybersecurity definitions of which the context vary based on sector and study area (Androjna & Perkovič, 2021; Meland et al., 2021). The complexity and broadness are illustrated in

Figure 3: visualisation of Cybersecurity extant . The vos-viewer colours show the occurrence and unpredictable nature of cybersecurity happening in cyberspaces and cyber-enabled systems. some studies argue for a unifying and interdisciplinary definition (Cains et al., 2022; Dan Craigen et al., 2014) urging that it is the best way towards finding a lasting solution. On the other hand, the complexity cannot be looked at from a general perspective since different sectors face different challenges hence complex definitions.

The risk perception in the maritime shipping is broad and complex topic (Afenyo & Caesar, 2023; Ben Farah et al., 2022; Cheung et al., 2021; Park et al., 2019a; Tusher et al., 2022a), and thus own complex definition as stipulated in the IMO page. 13. However, a multidimensional, concise, and universally acceptable definition opens a door to a great collaboration and understanding, which builds a strong foundation towards technological and innovation. Thus, a definition believed unifying was suggested by (Dan Craigen et al., 2014) as "The organisation and collection of Resources, Processes, and Structures used to protect cyberspace and cyberspace enabled systems from occurrences that misalign de jure from de facto property rights" (p.13. The definition is broken down in four (4) elements to illustrate unification and multidisciplinary illustrated in **Error! Reference source not found.**, including 1) the Organisation and Resources, stands for a complexity that cannot only be descriptive but rather show interactions with humans, humans, and systems and so on. 2) Protect cyber-space (CS and CS-enabled systems; this includes a broad protection for all threats including the untraditional aspect. E.g., intentional aspects, natural hazards, and aspects not viewed as cyberspace such as computer control systems and cyber-physical systems. 3) from occurrence-reflects unpredictability and that protection is intended to a wide range of intentional and unintentional occurrences and 4) that misaligns de jure from de facto property rights: any event that misaligns actual (de facto property rights) from perceived (de-jure) rights whether

intentional or accident is a cyber security incident. Definitions from other empirical sources are gathered in Table 1 where articles highlight definitions, details about possible causes and the remedies to cyber-attacks.

Figure 3: visualisation of Cybersecurity extant



Source: own construct

The definitions rotate around similar concepts but related to the industrial trend. For example, Cs in Maritime autonomous surface ships (MASS)- cyber physical, maritime infrastructure, information, and communication (Androjna et al., 2020; Ben Farah et al., 2022; Tusher et al., 2022a) The global navigation satellites systems (GNSS) are more susceptible to security threats and thus classification of threats are more frequently revisited. In addition, the valuation and security measurement and understanding surrounding legal framework, the change of mindset on threat landscape are among core steps to defining Cs (Chang et al., 2019; Cheung & Bell, 2021; Karim, 2022). In the centre of it a definition will only be descriptive if it rotates around processes and technologies. The human factor (Park et al., 2023c) and people should be on top of processes and technology (Ungkap & Daengsi, 2022a) because often they are sources of attack points to on board or off ship systems (Meland et al., 2021). To understand cybersecurity, there is need to be informed on knowledge, skills, and strategies of hackers. Confidentiality, integrity, and availability of sensitive data (CIA) are main concepts to internalise (Ben Farah et al., 2022), as they guide security policies in organisations. Confidentiality is the set of rules that limit information access, Integrity is the assurance that

information is trusted, and Availability is the guarantee of reliable access to information by reliable people. The three steps Identify, Gather and Map is suggested to facilitate the process.

Table 1: Summary cyber security themes

Article	Publication	Detail	Definition & remedy
Indetifying CS risks and control options for Maritime Chang et al., 2019)	IAMU- Conference	Lack of training, use of outdated system & being hackers target.	Develop a process, train, update, and upgrade.
Risk assessment for autonomous shipping Tusher & Munim (2022) - (Tusher et al., 2022b)	Maritime Economics	navigational systems more vulnerable	Communication systems to be clog free.
An assessment of Maritime CSR (Park et al., 2023a)	Ocean and coastal management	List top threats to direct efforts. Human factor is still on top	Evaluate risk levels of identified threats, then tackle those unacceptable. Define CS as a modern aspect
Aspects in Maritime cyber security (Afenyo & Caesar, 2023; Karim, 2022)	Ocean and coast management	In context of regulation, economics, training operation and data	Definitions should base on real time data
(Kuhn, Bicakci, et al., 2021; Ungkap & Daengsi, 2022a)	WMU Journal of Maritime affairs	Group Perception, response, and its impact to Cs risks- use of CS decision making exercise	Cyber space preparation- for robustness, Interrelations in people, technology, and processes
(Cains et al., 2022; Kavallieratos et al., 2020; Rahman et al., 2021)	IEEE-Informatics	Preservation of Confidentiality, Integrity, and availability of information	A resilient system functionality, maintenance of CIA

Source: own construct

The systematic bibliometric review study rotates around OT, IT and ICT and CI while relating cybersecurity, and weak points and targets within resilience -as illustrated above. Empirical such as, studies (Caines, 2020) found a similarity in their biggest study: context

driven, resilient systems, functionality and maintenance of CIA were the most influential to the definition of Cyber Security, while impacts of CIA vulnerabilities, probabilities of outcome were on cybersecurity Risks. With this backdrop, different disciplines seem weave definitions in own context depending on nature CIs.

2.3.2 Cyber security threats and Categories

Threats discussions in maritime shipping is very wide because of the reliance on IT/OT assets to support operations and manage data (e.g., collect, use, develop, receive, transmit and store) (Ben Farah et al., 2022; de Peralta et al., 2021; Kanwal et al., 2022; Meland et al., 2021; Oruc et al., 2022; Park et al., 2023c; Tusher et al., 2022b). ICT systems use data as information, while OT systems use the data to control and monitor physical infrastructures. The technology includes field controllers (i.e., GMDSS, GNSS, programable, etc..) network equipment, communication systems, hardware, and generally a complex infrastructure that makes it susceptible to vulnerability. These scholars urge the need for understanding CIs (OT &IT) and the potential attack points which in some cases may differ.

The threat scope is wide and ever evolves; Table 2 summarises threats and attack points and paths identified in this literature review. Scholars suggest, Paying attention to sectoral transition, economic impacts and insights as critical for cybersecurity awareness, for organisations to map where to prioritise their efforts (Ben Farah et al., 2022; Weaver et al., 2022); understanding threat types should begin with knowledge of most vulnerable components, critical dimensions and their interrelation (Ben Farah et al., 2022; Oruc et al., 2022; Park et al., 2023b; Tusher et al., 2022a) therefore threats vary in attack and impact. For example, cyberattacks categories in the port are in form of spear-phishing, distributed denial of services (DDos), social engineering, malware/ransom/trajons and port scanning. The DDos have several variations for example jamming attacks and hijacking are often seen in OTs such as AIS and ECDIS. The IBM 2023 threat reports and index (IBM, 2023, 2023), identify phishing, two years in a row as top cause for attackers breaking into organisations. Similarly concludes (Ben Farah et al., 2022; Park et al., 2023b). Therefore IT and OTs (Ben Farah et al., 2022; Kavallieratos et al., 2020; Meland et al., 2021; Park et al., 2023c; Tusher et al., 2022a) are constantly being studied in compositions to imagine the behaviours of hackers.

In a hybrid study identifying maritime Cyber Security Threats (CST) (Park et al., 2023c). Six list category ranking cyber security threats (CST) on criticality to maritime shipping was screened. Accordingly - Phishing, Malware Man – in the middle attack (MITM), Theft of credentials, Human factor and using outdated IT systems were rated. the study concluded that

Malware was the most critical threat category for the maritime and the vector source was the human factor. Understanding cyber risk types begins with knowing source identification. The AIS, IoT among others were critical paths where Jamming and spoofing were identified mostly (Androjna & Perkovič, 2021; Tusher et al., 2022a).However certain names of attacks categories were mainly observed in the review study the major one being Malware. Others are Phishing, Ransomware all appearing in different behaviour. Most threat types are classified under category Malware where ransom attacks are a biggest subcategory.

Spear- Phishing

This is created by emails containing suspicious links to obtain unauthorised access. They tend to be impersonation emails, often through attachments, links, or services (Ben Farah et al., 2022; IBM, 2023, p. 4). The email often confuses to be from a trusted link to an extent that even an experience person may be confused. It takes an employee to klick on the link and so the organisation is jeopardized, because all the information will be transferred to the hacker after accessing the information system. The hacker installs key- loggers to capture passwords and logins and determine the identity of company staff. Sea crews and other maritime personnel using personnel devise could receive phishing emails or visit malicious websites and thus installing the viruses on the ship operating systems (Ben Farah et al., 2022; Meland et al., 2021; Park et al., 2023a). A separation of passwords and logins for crew and vessel is suggested especially in this case.

Malware/ransom/Trojans

This category is often directed to the server and information systems. Increasingly a common place is through malicious Microsoft office documents, usually attached to phishing emails and macros (Ben Farah et al., 2022; Meland et al., 2021; Park et al., 2023a). The developers created these malware macros, that accesses open documents or damages devises without the knowledge of the user, by downloading files from infected websites, connecting USB drives, and removable media that has malicious malware (Park et al., 2023a), the result is either ransomware, trojans or distributed denial of service (DDoS); refusing access to a physical infrastructure. watching out for newer malware tactics (e.g html files, macros and password compressed files and many others) is suggested. Scholars listed malware since as a big threat to shipping environment given the fact that it is likely to access and damage vessel systems or robe sensitive information. There are various cases in the maritime sector that are linked to malware; for example the latest; 2023 ransom ware that hit the servers of a classification society

in Norway affecting customers 'vessel systems following the shutdown (Garry, 2023), the Not Petya- Maersk encrypted malware that attacked computer systems both in Europe and India (Ben Farah et al., 2022; Meland et al., 2021), that demanded USD 200 million to give access. Lists of maritime cyber-attacks with malware repeatedly on top ten is availed (Ben Farah et al., 2022; Meland et al., 2021; Park et al., 2023c) . The top 10 threats- malware in a period of 2010-2020 is provided by Meland et al. (2021), Ben Farah et al (2022) list threats and their typical attack vectors and the latest from Park et al. (2023). Malware is still highly ranked, and mitigation is needed. DNV`s ransomware and Port Lisbon "lockbit" ransomware (Garry, 2023; Techcrunch, 2023) are 2023 latest attacks that add evidence to scholarly works.

2.3.3 Human factor / social engineering:

These attack categories depend on exploitation of human curiosity to advance a malicious act (Ben Farah et al., 2022; Meland et al., 2021) and the cognitive attitude based on either 1st or 2nd century; to creating cyber security awareness (Ungkap & Daengsi, 2022b). In determination of factors and measures associated with employees cyber security awareness in a transport sector, understanding the human factors- based on individual differences (cognitive, education, experience) is required to gain their level of cyber awareness. Social media or instant messaging usage patterns are means for hackers to gather information, so the behaviour of employees on these platforms are worth being clear over. For example, a hacker can obtain critical information through Facebook, Instagram or Tik Tok. Other social engineering attacks include Baiting and Quid Pro Quo (Ben Farah et al., 2022). Meland (2022), lists 14 incidents that are causes of economic fraud linked to social engineering of which human is crucial.

2.3.4 Man in the middle (MITM)

This as the name sounds is another unknown intruder in between two different parties, that collect information in pretence of being one of the parties involved. This hacker hides in open WIFI's /hotspots or fake websites and prevent users from sending and receiving or even redirect information to another user (Park et al., 2019b, 2023a; Thomas, 2022). An illustration of threats and categories is summarised in Table 2 based on review studies.

Table 2: Threat category

Threat/Category	Vulnerability	Attack-paths	**Attach points**

Malware: *Ransom, not petya,DDOs:* (Barker et al., 2022; Ben Farah et al., 2022; Meland et al., 2021; Park et al., 2023c)	Communication links: Via unencrypted WIFI, an attacker inserts themselves to control and change a conversation, between two parties unknowingly, and demand payment.	Files, macros, html	GMdss, GNSS, CCTVs, VHfs, crews, AIS
SpearPhishing: Emails, Ryuka: (Meland et al., 2021; Park et al., 2023a)	Accessing impersonated emails e.g., banks, insurance companies and other sources that seem trustworthy	USB, email, attachments, PDFs, remote desk protocol	Crews, operators, AIS
Man In the Middle (MITM) (Cheung & Bell, 2021)	Via unencrypted WIFI, an attacker inserts themselves to control and change a conversation, between two parties unknowingly.	Ransomware , ship servers	
Theft of ID:(Duzha et al., 2017)	Using automatic logins, giving personal information to fake sources	AIS, links, transactions, spoofing, general links	
Human factor/social engineering (Androjna & Perkovič, 2021; (Meland et al., 2021)	Employees may lack knowledge on new CS threats. Companies too may lack procedures	Data breaches- Tik tok, facebook (SOME)	
Outdated ICTS ((Meland et al., 2021)	Use of expired firewalls and antivirus software		

Source: own construct

2.4 Mitigation of cybersecurity threats

The concept of Mitigation is a risk management concept used at providing a holistic solution in regard to the evolving cyber risk environment with a focus on collaboration with maritime supply chain actors and stakeholders (Barker et al., 2022; Cheung et al., 2021; Duzha et al., 2017) . To mitigate is to reduce economic consequences which are the main target of malicious attacks and is enhanced by real time data. However, it is not that easy. There is a challenge of getting real time logs about the attacks and how they are delt with in maritime supply chain (Cheung et al., 2021). The national institute of standards and technology cyber security framework –NIST CSF 1 – voluntary a world leader from the US in creating critical

solutions, was suggested with components encouraging collaboration to aid identification and assessment for mitigation (Barker et al., 2022; Duzha et al., 2017, p. 250) . NIST is a voluntary framework that consists of standards, guidelines, and best practice to manage cyber risk. It builds on 5 sequencies; Identify, protect, detect, respond and recover (Barker et al., 2022, p. 22).

To Provide such a holistic solution, it requires, collaboration and transparency in the cyber community. Mitigate framework emphasises the collaboration of various stakeholders in identification, assessment and mitigation of risk associated with cyber assets and international maritime supply chain processes. This is through risk management, advanced simulation, visualisation of potential cyber-attacks and open intelligence services among others according to (Duzha et al., 2017). Such a radical shift requires 8 components assumed to complement each other.

- ⇒ Asset modelling and visualisation, in this component each user (maritime stakeholder and supply chain participant) follows strict rules to declare their cyber assets along with possible mapping of related risks.
- ⇒ A modelling software that allows analysts to keep track of own possible tried models and allowing to provide mapping of threats.
- ⇒ Simulation- to help discover attach paths given a particular security mapping and offering best defensive strategies.
- ⇒ Collaborative risk assessment that makes it possible to conduct assessment.
- ⇒ Open interagency to provide near real time data.
- ⇒ Notification and reporting components to inform users of any concerns.
- ⇒ An administrative component to track all administrate related issues.
- ⇒ An access control and privacy components

Although the Cyber security mitigation developments within maritime are still perceived sluggish in comparison to other sectors (Afenyo & Caesar, 2023; Kanwal et al., 2022; Karim, 2022; Kuhn, Bicakci, et al., 2021; Lloyd`s Register, n.d.; Tusher et al., 2022a). There seem to be some novel risk management systems in pipeline, and more studies are identifying other possible ways to mitigate risk. However, a complex legal system, challenges novelty, as well as challenges on disclosures on risks and the different methods that fail to intertwin.

2.4.1 Rules and regulations.

To improve cyber resilience in maritime shipping, the international Maritime authority has (IMO), came up with recommendatory guidelines for assessment and development of threat

procedures (Msc-Fal.1/ Circ.3) (IMO, 2017a). The stakeholders - ship owners and managers through their company`s management systems, in line with ISM and ISPS codes (IMO-ISPS, 2021), supported by IMO resolution MSC. 428 (98)[5], have a duty to assess, develop and implement relevant measures in harmony with relevant national, international, and flag state rules and regulations (IMO, 2017a; Kanwal et al., 2022).

These guidelines follow a five-step framework of the United States National Institute of Science and technology (NIST) but can be followed non-sequentially. Elements include Identification, Protection, Detection, Response and Recovery. Identification requires, defining personnel roles for cyber risk management, and identify systems according to risk level. Protection is to implement risk control measures and plans to protect against the threats. Detection is about implementing ways of detection in a timely manner in case a threat hits. The Response is about developing and implementing activities that enhance resilience, and restoration in case of a threat. Lastly the recovery is identification of back up and restoration measures in aftermath of the attach of the system.

2.5 Cyber risk frameworks

The adoption of risk frameworks is widely discussed, and adoption depends on the risk at hand. For example, Ransomware, is a very big problem of which an individual framework is discussed (Barker et al., 2022). These discussions are grounded on NIST -a framework for improving critical infrastructure cyber security. Which was also adopted by IMO. The NIST stands for National Institute for Standards and Technology NIST since 1901 previously known as bureau of standards, a living document constantly being updated in versions such as version 2.0 (NIST, 2022). This framework is an alignment of functions, categories and subcategories with the business requirements, resource availability and risk tolerance.

The framework adopted depends on the risk exposure. Ransomware is identified a leading threat in the maritime, where the attackers ask for big sums of money thus, NIST framework for ransomware can be applied to build own (Barker et al., 2022). Organisations are advised to follow recommended steps to prepare for and reduce the potential of successful ransom attacks the cyber security framework has these following steps:

- Identify: develop an organisation understanding for everyone to understand the context of cybersecurity and the possible attacks. Understand the business and the resources that support critical functions.

[5] https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

- Protect- is to develop appropriate safeguards. Through trainings,
- Detect- is to develop and implement appropriate activities to identify the occurrence of cyber security.
- Respond- develop appropriate solutions to the detected issues.
- Recover- develop plans to reinstate after occurrence, and it is better to be real time.

The above 5-step framework provides an inventory list of safety and business-related critical system and software These together are the pre-requisite to execution of a cyber risk assessment. The current industry practice requires documentation of compliance. The IMO policies and requests are still challenging (Afenyo & Caesar, 2023; Kanwal et al., 2022; Karim, 2022; Kuhn, Bicakci, et al., 2021) such that a captive system can be vital.,

2.6 Categorization of Various Measures

The frameworks of NIST and DVGL, illustrate a fact that there are different ways of categorising defence actions. This is similar in the literature that selected out different approaches too (Cheung & Bell, 2021; Enayaty-Ahangar et al., 2021a). According to Enayaty-Ahangar et al.,(2021) six mission areas based on NIST are studied; with a three group undercategory. The basis of undercategory is Defence Action Intention (DAI) - or missions if you will. They are further divided into – Before/Pre, During/Real-time or After/aftermath. The Before involve mission areas whose defensive actions are taken prior to attack i.e prevention and mitigation. The during/real-time, are mission areas whose required actions take place during or after the incident. Forexample respose and detection. The after/recovery, are mission areas whose required actions occur after the attack, for example recovery. These missions are also Similar to Cheung & Bell, (2021) cartegorisation as they together support the proactive planning, real time opertional planning and recovery planning as important categories.

1. The precautionary measure is the pre-requisite to cyber-attack defence and are implemented before the attack occurrence.
2. The real-time recovery calls for the defensive action plans carried out amidst the cyberattack.
3. The aftermath measures are implemented after the cyber-attack.

Prevention is to avoid any circumstance that can lead into any risk. However, alone are preventive measures insufficient towards cybersecurity threats since the attackers will eventually find out how to get to their target. Improvising other plans is suggested (Cheung &

Bell, 2021; Enayaty-Ahangar et al., 2021a), especially starting with risk identification and vulnerability assessment (Park et al., 2023a). As a hint to enterprises implementing effective CS measures, Donaldson et al., (2015) makes it concrete on having multiple measures to handling cyber-attack- prevention alone is not enough without detection (p148-149). What makes up an effective cyber security? According to (Donaldson et al., 2015), one cannot rely exclusively on technologies, such as walls, doors, and gates to stop attackers. By Adding a detection to the security profile, an enterprise will at least catch the attack in progress and have an opportunity to stop it; once stopped, the avenue can be blocked, closed and the vulnerabilities the attackers were exploiting disrupted. There is a consensus indeed that a determined attacker is unstoppable with preventive measures alone however long the list may be. This explains the case of high-profile attacks leaves no doubt prevention needs a combination of planning phases and categories (Cheung & Bell, 2021; Enayaty-Ahangar et al., 2021a). Let us navigate them below.

2. 6. 1 Precautionary measure

As discussed in the previous section, legal framework is an important precautionary measure. A basis of various frameworks (Kuhn, Kipkech, et al., 2021; McNicholas, 2016). The various standards are ranging from national guidelines, to sectoral and global based on updated legal policies and regulations. It is thus suggested to plan according to available industrial frameworks while building up basic cyber security processes (DNV, 2023; McNicholas, 2016, p. 300). Regulations and companies' procedures are often widely discussed in literature (Cheung et al., 2021; Enayaty-Ahangar et al., 2021a) as important instruments, if updated in relation to the risks pace. Empirical studies (Afenyo & Caesar, 2023; Burrell et al., 2020; Cheung & Bell, 2021; Kanwal et al., 2022; Karim, 2022; Kuhn, Bicakci, et al., 2021), evaluated cyber preparedness through, regulations, company procedures from managers, procedures from shipboard system readiness, training and awareness, human factor, and compliance. Regulations positively affected cybersecurity related procedures such as training and awareness- thus leading to readiness (Kanwal et al., 2022).

On the other hand, complexity of regulatory frameworks can be a hinderance to understanding companies' safety management systems (Afenyo & Caesar, 2023) if not simplified to stakeholders. With human factor, bearing a high risk level to cyber security in logistics and maritime supply chains (Ben Farah et al., 2022; Burrell et al., 2020; Kanwal et al., 2022; Meland et al., 2021; Park et al., 2023c), Training is vital. Infarct there is clear evidence that absence of structured security awareness training for employees is a major source of

vulnerability. A security plan involving employees at its construct phase is suggested (Ben Farah et al., 2022), to ensure that procedures are more than tick off boxes to compliance. The technological giants also remind the on integration of people, plans and technology as a vital precaution.

Additionally measures to ensure CIA- confidentiality, integrity and availability are precautional (de Peralta et al., 2021). Whereas there is a consensus that 100% cyber risk reduction is impossible (Meland et al., 2021; Park et al., 2023a), a risk analysis plan, focusing on those with unbearable risk and manageable is a good start to risk mitigation(Ben Farah et al., 2022; Carnival, 2023; Cheung et al., 2021; Maritime Executive, 2023; Meland et al., 2021; Park et al., 2023c; Tusher et al., 2022a). Literature indicates often applicable measures such as access controls, trusted firewall and gateway installations, regular updating, counterfeit prevention, segregated WIFI in case of passengers and crew. In maritime supply chains, as part of supply chain management, due diligence is vital. Information sharing, supplier auditing and supply chain partner collaboration are vital measures for stakeholders to maintain supply chain network availability and connectivity (Burrell et al., 2020; Cheung & Bell, 2021) to enable risk identification which also creates a sense of responsibility to everyone involved. This goes in line with training of personnel, developing an internal culture on risks such as whistleblowing all to create awareness.

Furthermore, a common approach is the installation of software that detect the risks (Ben Farah et al., 2022; Meland et al., 2021). These must however be certified and from trusted vendors (IBM, 2023). For Maritime corporations such as Saipem an Italian subsea and oil company and Carnival (Carnival, 2023), risk detection mitigated potential losses. Saipem was able to contain the attack while at their regional servers in the middle east giving them time for backups. It was also upon detection of the risk in Carnival that a launch of investigation was undertaken that saved the corporation.

Another measure identified in the literature is data protection through updates of software, having antiviruses and separation of internet logins (Ben Farah et al., 2022; Kanwal et al., 2022; Meland et al., 2021). The fact that cyber incidents result into data leakage, most sources were concerned on data protection where the most dominant technology under discussion was block chain, IoT, among others and a separation of crew logins from the vessel login. However, updates can also increase risk of attacks; if it is done through removable media, as this is often means to install malware; a file used by hackers to obtain system access.

Lastly but not least, the use of password is the widest applicable precautional measure. Industrial experts and scholars advise on a good password policy as an essential cybersecurity

measure if it conforms to the following yardsticks: it should be hard to guess, avoid using private data such as own birthdays, not to use on multiple accounts, using two/ three factor authentications, and regular updates. Overall, there are a variety of precaution as illustrated in table below.

In table a summary of various measures considered precautionary based on review studies is provided. Identifying precautions as main category with types of measures as the subcategory.

Table 3: Precautions to mitigate cyber security risks.

Category	**Measures**	References
⇒ Precautionary actions	Rules, Regulations, procedure	(Becmeur et al., 2017; Kanwal et al., 2022; Kuhn, Bicakci, et al., 2021)
	Access control, detection, and strict policies	(Ben Farah et al., 2022; Meland et al., 2021)
	Certified hardware and software, 3pp	(Meland et al., 2021; Park et al., 2023a; Ungkap & Daengsi, 2022b)
	Supplier due diligence	(Burrell et al., 2020; Cheung & Bell, 2021)
	Counterfeit prevention	(Carnival, 2023; Maritime Executive, 2023)
	Firewall and gates	(Kavallieratos et al., 2020)
	Staff and crew training, awareness, Internal controls	(Afenyo & Caesar, 2023; Androjna & Perkovič, 2021; Becmeur et al., 2017; Ben Farah et al., 2022; Kanwal et al., 2022; Kavallieratos et al., 2020; Meland et al., 2021; Park et al., 2023c)
	Outsourcing to 3PPs	
	Regular patching	(Kavallieratos et al., 2020)
	Updating antivirus	(Ben Farah et al., 2022; Kavallieratos et al., 2020; Park et al., 2023c)
	Standards- ISOs	(Ben Farah et al., 2022)
	Supply chain partner collaboration	(Burrell et al., 2020; Cheung & Bell, 2021)
	Information sharing, collaboration	
	Whistleblowing	(Burrell et al., 2020)

	Component assessments	(Oruc et al., 2022; Tusher et al., 2022a)
	Manual technics	(Meland et al., 2021; Park et al., 2023a)
	Strong password policy	(Meland et al., 2021; Park et al., 2023a)
	Segregated WIFI	(Ben Farah et al., 2022)

Table: Own construct

2.6.2 Real- time Recovery

While there is a variety of literature on precautionary measures, real time is limited (Cheung et al.,2021). Amidst the attack, measures are undertaken to prevent the worst-case scenarios (Ben Farah et al., 2022; Carnival, 2023; Maritime Executive, 2023; Meland et al., 2021). To prevent further damages several other key systems are shut down for example (IMO sophisticated attach, DNV, Carnival and Saipem) applied a similar tactic during the attack. Previous review mention component recovery, component isolation, real- time monitoring, collaboration and interaction within supply chains and a task force (Cheung & Bell, 2021; Enayaty-Ahangar et al., 2021a). Even though managers may prefer to keep information reporting to a minimum due to confidentiality and integrity (Ben Farah et al., 2022),The IMO guidelines requires stakeholders to immediately report the incidence to security and police administration.

Reporting is important as it gives more information to the task force to mitigate data loss (Carnival, 2023; Maritime Executive, 2023; Meland et al., 2021) The shutdown of the system and its servers (Ben Farah et al., 2022) – as practiced in the malware attack of Mediterranean Shipping company in 2020 contributed to mitigation of data loss that would have been grotesque, as shutdown contained the hacker is a particular area instead of reaching all systems at once. Another one is, System abandonment of infected physical infrastructure, or even to allocate tasks forces who work effortless to recover systems back to function. In other incidences a whistle-blower (Burrell et al., 2020) for precaution, and incident report during and after is much useful; it gives an indication on the hacker behaviour that can be used as a reference. There should also be controls and procedures in place to inform customers affected-lack of security strategies is still a main cause for a number of attacks (Ben Farah et al., 2022;

Meland et al., 2021). In table below, a summary of various measures considered real time based on review studies is provided.

Table 4: Real-time recovery to mitigate cyber security risks.

Category	**Measures**	References
⇒ Real-time recovery	Component isolation	(Ben Farah et al., 2022)
	Real time monitoring	(Ben Farah et al., 2022; Meland et al., 2021)
	Shut down and isolate	(Ben Farah et al., 2022; Carnival, 2023; Meland et al., 2021)
	Supply chain interaction	(Burrell et al., 2020; Cheung & Bell, 2021)
	Vulnerability identification	(Ben Farah et al., 2022; Burrell et al., 2020; Cheung & Bell, 2021)
	Task force	(Barker et al., 2022; Carnival, 2023)
	Behaviour Analysis and feedback	(Ben Farah et al., 2022; Cheung & Bell, 2021)

Table: Own construct

2.6.3 The aftermath

At the end of the attack, there is need for system/ server recovery hence after math measures are necessary to refine the pre-implemented precautionary and real- time recovery measures (Ben Farah et al., 2022; Cheung & Bell, 2021; Meland et al., 2021; Park et al., 2023a). The affected systems need to be immediately reinstated to full functionality. If data is disrupted, immediate backup is undertaken for restoration. Organisations are urged to have data restoration protocols to enable this practice. In a maritime supply chain, collaborative recovery plan implemented with other stakeholders is essential for a complete and rapid recovery along the entire maritime supply chain (Barker et al., 2022). Also, resilient infrastructures are essential in speeding up the recovery speed. For example, geographically distributed data locations, virtual networks, reliable cloud computing services, uninterrupted power banks, and stable storage (Cheung et al., 2021, p.9). Data backups saved an Italian oil field company-Saipem which would have otherwise lost everything when their 400 servers in the middle east were attached (Meland et al., 2021, p. 523).. The company also undertook diagnostic measures including shutting down their server.

The management of ICT is helpful in reduction of the damage caused by hackers. and is a set of defensive measures to identify technology, processes, and people responsible for attacks and infiltrations against assets that violate the CIA of these assets, and using this

information to diagnose, contain and recover from incident (Barker et al., 2022). A summary of various measures considered Aftermath based on review studies is provided below Identifying aftermath as main criteria with measure types as the sub criteria.

Table 5: Aftermath measurers to mitigate cyber security risks.

Category	**Measures**	References
⇒ Aftermath	Data backup Diagnosis	(Maritime Executive, 2023; Meland et al., 2021)
	Collaborative recovery plan	
	Information security incidents reports	
	Insurance	(Ben Farah et al., 2022; Cheung & Bell, 2021; Kapalidis et al., 2022; Meland et al., 2021)
	Resilient system designs	(Cheung & Bell, 2021; Enayaty-Ahangar et al., 2021b; Tusher et al., 2022a)
	Vessel audits	(Kechagias et al., 2022) Peralta

Table: Own construct

As discussed above, through the suggested three planning categories (Cheung & Bell, 2021; Enayaty-Ahangar et al., 2021a); before, during and after the threat damage on to organisation or entire supply chain may be combatted. However, studies seem to mostly focus on preventive measures other than real time recovery and aftermath. To further understand threat mitigation, it is a great step looking for mitigation frameworks that resonate with security compliance and regulations such as ISPS, ISO27001, ISO27005 and ISO2800 (Barker et al., 2022; Duzha et al., 2017) reason being, they are collaborative and interactive. These base from NIST which is a world's biggest voluntary threat mitigation framework

CHAPTER THREE: METHODOLOGY

3.0 Chapter Overview

Scientific research can be described as a collection of information on a phenomenon with a purpose of contributing to science. It includes a systematic collection, interpretation and evaluation of data aiming at providing new knowledge (Creswell & Creswell, 2018; Frankfort-Nachmias et al., 2015; Sekaran & Bougie, 2019). The aim of methodology chapter is to guide readers understand the study mapping.

3.1 Research design

The research design explains the study plan, research instruments data collection and reliability, validity, and ethical considerations. Is a strategy that guides the contextualisation of the study topic, through a comprehensive planning process regarding data collection and analysis. A research design can have three levels; posing a question for examination, collecting the necessary data, and presenting the findings to answer the research question. A descriptive research design was opted for in this case as will later be seen in questions and data collection.

3.1.1 Research Method

This study received answers to questions regarding **Cyber-risk perception and mitigation strategies within maritime shipping** by use of a survey method. The purpose of using quantitative method is to discover a phenomenon assumed to exists and try to explain it through numerals. This method enables numeric data and considerable samples be considered as population representative. It relies on objectivity and is an appropriate method to use when collecting quantifiable measures from samples of the population. Furthermore, it seeks to obtain accurate and reliable measures that allow statistical analyses Quantitative data and statistical data analysis is preferable (Creswell & Creswell, 2018; Frankfort-Nachmias et al., 2015). Analysis such as descriptive statistics, frequency distribution, one-way Analysis of variance (Anova) Chi-square, and t-tests were performed by use SPSS software, because the data was descriptive.

3.2 Sample and population

The study requires data collections from subject matter experts (SMEs) (experienced in maritime and directly affected e. g Academicians, managers, and seafarers). Several studies indicate vulnerability of seafarers, and it is believed that a combination with subject matters would yield valid knowledge. Thus, receiving reliable and valid answers to the question necessitated relevant respondents. The study population included various maritime enterprise sizes as in table on page 35. The enterprise sizes were defined based on Eurostat- an online scientific research database that explains statistics and sizes (Eurostat, 2023). Small companies were 10-49 employees, medium 50-249 while large were 250 and above. Cybersecurity risks are more related to bigger companies, as they are targets to hackers for economic and other various reasons discussed in section two 17 hence our target as well. Thirty (30) participants from managerial and seafarer background within maritime related firms were reached. Table Table 6 and Table 7 show 22 usable, and consisted of 8 shipowners, 4 seafarers, 7 others, 1 maritime insurance and from Academics.

3.2.1 Sample strategy

A purposive, convenient and snowball sampling strategy (Clarksons, 2021; Frankfort-Nachmias et al., 2015) was opted for as explained below. Participants were chosen on purpose for their professional experiences and knowledge, via LinkedIn which was convenient. Through snowball, they were requested to further recruit relevant participants in own network. The researcher drew in own LinkedIn profile to reach participants. The planned sample was thirty (30) seafarers and ten (10) managers. It was a plan that managers would share these surveys further to seafarers. The result is illustrated in Table 7**.** Although seafarers seem less represented, sample illustrated on page 38 representative.

Table 6: Company and organisation types

Variable	Category	Frequency	Percentage
Company type			
	Shipowner	8	36.4%
	Maritime insurance	1	4.5%
	Seafarer	4	18.2%
	Academics	2	9.1%
	Others	7	31.8%
	Total	22	100

Table: Overview Participants

3.3 Data collection Procedures

Data collection entails facts presentation to a researcher from respondents (Frankfort-Nachmias et al., 2015). To meet intended objectives, pre-conversations, systematic literature review, bibliometric analysis, conversations with SMEs, guided survey preparation and conduct in the study. In otherwards multiple groups were sent the structured survey questionnaire illustrated in A171. Due to design of descriptive nature secondary data and questionnaire survey were parallel. The was sparked off from various scholarly articles, such as Cheung, Bell, and Bhattacharja (2022) which laid a foundation for some replication. This bibliometric study identified and categorised risks and measures in logistics and supply chain as; realtime recovery, aftermath and precautionary as seen on page 27. For more contribution on a similar problem, in a Maritime shipping context, this thesis aims to extend the knowledge search by combining bibliometric studies and the survey of SMEs.

3.4 Web Survey

The web survey method of data collection is increasingly used in research for its reliability and flexibility(Frankfort-Nachmias et al., 2015). The use of online/web surveys for their efficiency in data collection and flexibility for the researcher makes it easy to adopt to according to Frank-Nahmias et al. (2015). Recent Studies have adopted web survey for example Tusher, Munim, Notteboom & Nazir (2022), who used LinkedIn web survey as part of their data collection in their study regarding Cyber security risk assessment for autonomous shipping (Tusher et al., 2022a). The process was directly undertaken with some assistance of perusing through SMEs. Based on this literature study, a web-survey with choice and Likert scale questions was created and distributed using university of Oslo`s nettskjema (UIO, 2023) in a period June – August 2023.

3.5 Questionnaire and Survey administration

We first pre-tested the questionnaire to investigate validity and reliability of content in different procedures based on Churchill (1979) a known classical for– a paradigm of developing better measures. Firstly, the questionnaire was sent to an SME who assessed content validity of each question in terms of clarity, readability, and universal adequacy for representing cyber-security and mitigation concepts. Secondly, it was circulated to other external valuable experts who provided feedback on design, settings, and structure. After receiving the feedback, questions considered ambiguous and lengthy were amended to avoid vagueness and misinterpretation. The improved version was then ready with a cover letter explaining the study

purpose as see in A1- 71. The reliability of the instrument was also tested to ensure reliable quality. The improved version was then sent to maritime acquaintances in our sample frame. On each questionnaire was a brief explanation clarifying the approach to ease respondents understanding. We kept track in a spreadsheet administering, tested both on mobile screens and sending to own self to see how it would appear.

The questionnaire was divided in five sections A-E on page 71, with a combination of Likert – point scales under each section. Respondents were requested to review each statement and provide their level of knowledge as the Likert points suggest. The sections were – Section B: knowledge on cyber security incidents C: knowledge on cyber security risks, D: Knowledge on cyber security procedures and E: knowledge on cyber security mitigation procedures. Several questions regarding background were also incorporated in section A, within recommendations from Norwegian Agency for shared services in education and research (SIKT)[6] originally NSD.

3.6 Validity

To ensure adequate data collection that is representative for the research, informal conversations are undertaken with six (6) subject matter experts (SME) in the beginning of this research, and attendance of Cyber security conference for maritime and energy sector. The SME were Security and IT managers (2) for; a publicly noted shipping company, a crew management company, Energy company in maritime supply, Maritime insurance company and a global IT security company. In addition, were conversations with crew managers (2). This process was helpful along with the literature. To follow up on response rate, kind reminders were sent every after two weeks. Towards the end of data collection, a separate copy link was sent to a particular single company where the researcher received extra response.

3.7 Ethical considerations

To ensure anonymity of respondents, personal data protection procedures based on SIKT were followed. Participants were recruited through snowball, purposive and conveniently by use of researchers LinkedIn network and workmates within maritime without characteristics for personal identification as described by NIST.

[6] https://sikt.no/en/about-sikt- Norwegian agency for shared service in education and research is former NSD.

CHAPTER FOUR: FINDINGS

4.0 Chapter Overview

This chapter presents survey findings undertaken June -August 2023. The presentation follows the survey questionnaire in appendix A-171. The chapter opens with general findings and then proceed to sections based on questionnaire sections.

4.1 General findings

Out of 98 contacts to whom questionnaires were sent, thirty usable ones were received from SMEs making response rate 31%. We started with data cleaning by excluding empty lines, spaces, and converting texts to numbers. We ran straight lining by standard deviation in the excel and the validity was justified thus leaving n=22 usable respondents. A sample demography in Table 7 presents company type, gender, position, education level, work experience and location of 22 respondents. The population was n= 22 of which eight (08) were shipowner/operator, one (01) maritime Insurance, four (04) seafarer, two (02) academics and seven (07) who never specified (others). Shipowners were highly represented with 36.4% as well as seafarers 18.5% and unspecified with 31.8%.

4.2 Background Information

The ship owner represents the biggest percentage of the data (36.4%) and when added with seafarers (18.5%) makes the sample representative of maritime. The (9.8% from academics also adds weight due to the knowledge they possess, Academicians were PhD the others (31.8%) are also from maritime although never specified their roll ref Information Table 7 and A-1. There seem to be an even gender distribution where men are 59% and women 40.9%. The positions were mainly managerial; crew managers (13.6%) and engineers; 18.2% dominated besides the unspecified – 59%. Respondents worked in seven locations and worldwide. These included Norway (68.2%), Denmark (4.5%) USA, Philippines (4.5%), Bahrain (4.5%), Uganda (4.5%), worldwide (13.5%) and onboard research vessels (4.5%). Norway was dominant.

Table 7**: Overview of respondents**

Variable	Category	Frequency	Percentage
Company type			
	Shipowner	8	36.4%
	Maritime insurance	1	4.5%
	Seafarer	4	18.2%
	Academics	2	9.1%
	Others	7	31.8%
Gender			
	Male	13	59.1%
	Female	9	40.9%
Position			
	Class. Society rep.	1	4.5%
	Crew manager	3	13.6%
	Manager Eng. navy.	4	18.2%
	seafarer oper.	1	4.5%
	Others	13	59.1%
Education level			
	PhD	3	13.6%
	Master	7	31.8%
	graduate	8	36.4%
	High school	4	18.2%
Work Exp.			
	0-5 years	2	9.1%
	6-11 years	4	18.2%
	12-15 years	2	9.1%
	15++	14	63.6%
Location			
	Norway	15	68.2%
	Denmark	1	4.5%
	USA	1	4.5%
	Philippines	1	4.5%

	Bahrain	1	4.5%
	worldwide	3	13.5%
	Sci. research vessel	1	4.5%
	Uganda	1	4.3%

4.3 Findings and results

The Appendices 2-571 illustrates visuals from SPSS that were based on to construct and present findings and analyses. The mean and standard deviation are used to explain the findings based on the following score intervals: 1.0-1.8= Strongly Disagree, 1.90-2.60 =Disagree, 2.70-3.40= Neutral, 3.50-4.20 =Agree and 4.30 – 5.00 Strongly Agree. In addition to sample background above, this section presents analyses following parts of the survey responses.

1. Knowledge on cyber security incidents
2. Knowledge on cyber security risks
3. Knowledge on cybersecurity procedures
4. Knowledge on cybersecurity mitigation strategies
5. Security mitigation strategies and types of attacks
    a) Rating of preventive strategies in organisations
    b) Strategies undertaken during the attack.
    c) Strategies undertaken after the attack.

Cyber security perception is guided with questions 1-4, whereas mitigation is guided with questions 5a -d.

4.4 Knowledge on Cyber security incidents

The start was to rate respondents' cybersecurity knowledge level. Seven questions (see A-2) on page 71 on five points Likert scale were used. Respondents were requested to indicate their view using the scale where; 1= strongly disagree, 2= Disagree, 3=Neutral, 4= Agree and 5= Strongly Agree. The mean and standard deviation were used further to explain the findings.

Table 8: **Descriptive statistics on knowledge about cyber security incidents**

Item	N	Minimum	Maximum	Mean	Std. Deviation
Malware attacks	22	2	5	4.27	.827
Phishing knowledge	22	2	5	4.05	.899
Social engineering	22	2	5	3.77	1.020

Data breach consequences	22	3	5	4.55	.596
Suspicious mails recognition	22	4	5	4.45	.510
Fake websites	22	2	5	3.73	.827
Unsecure networks	22	2	5	3.68	.945

Source: own construct (survey)

Figure 4: Most familiar cyber threats

1 = Strongly disagree, 2= Disagree, 3 =Neutral, 4 = agree, 5= Strongly agree

Findings indicate four areas where respondents demonstrated most awareness. Data breach consequences with a mean score = 4.45 and std = .596, suspicious email with mean score = 4.45 and std =.510, malware attacks with mean score 4.27 and std = .827 and Phishing with mean score = 4.05 and std =.899. Data breach had the highest mean scores as well as most significant, followed by suspicious mail recognition. The unsecure network had the lowest mean score. A mean score comparison was also done on different sample aspects. We wanted to find out whether there was a difference in male and female awareness on high scoring variables (data breach, suspicious mail, malware, and phishing)- A-2b. The 9 female participants demonstrated more awareness compared to 13 male participants about data breach consequences (mean, 4,56, std. 0.0726) and phishing (mean 4.22). For the male, a slight difference in mean scores was observed in Malware and social engineering awareness (mean 4,38 vs 4.11) and (mean 3.85 vs 3.67). Another means comparison was regarding work experience- A-2 d. The newly employed (0-5 years) seemed most aware of data breach (mean,4.50). Those between 11- 15 years in work demonstrated an average awareness on all

aspects. However, those with a work experience 15++ surprisingly seemed not aware of all aspects. The awareness based on education level (A-2. d) does not indicate a significant difference between High school (HS), graduates (grad), masters (Ms), apart from the PHD on malware and social engineering with mean scores and std (4.00, std 0.000). Based on positions (A-2. e), 3 crew managers seemed less aware on the three aspects- malware, phishing, and social engineering (mean score 3.67). At this level, cyber security threat awareness was of relevancy to gender – where women and men demonstrated different threat awareness, working experience - where new employees demonstrated more awareness compared to longer serving employees and positions held. However, the levels of education were of no relevancy.

Further analysis was done by use of one sample t-test and independent sample tests and 1-way anova. Gender significancy in relation to knowledge of cyber security incidents in all the seven variables - A-2b71 was tasted through a t-test. In all cases significancy was not observed because all the p-values as based on 2- sided p test were greater than 0.05 ($p>0.05$). Further robust analysis was undertaken through one-way Anova to test the differences in more than two groups` mean scores in a categorical variable. In this case the researcher looked at mean scores from category education, for 4 groups, i.e., high school (1), graduate (2) MSc (3), and PhD (4). There was no significant relationship in the education level and cyber incidents knowledge level as showed by p- values; 0.620, 0.324,0.260, 0.980, 0.842, 0.620 & 0,862 respectively in A-2 d. At the end, in an overall analysis there was no difference neither by gender nor education level in relation to cybersecurity knowledge in our sample.

4.5 Knowledge on Cyber security risks

This section comprised of 5 questions to measure respondents` cyber risks knowledge level. Likert scale was used with points 1 to 6, where by 1 was no knowledge at all, 2 slightly, 3 moderate, 4 very confident. The questions asked included how confident you feel in identifying cyber security risk, how often do you update your passwords for your online accounts, how familiar are you with common security risk such as phishing, malware and ransomware, how often do you back up data and how frequent do you review privacy settings on social media and other online accounts.

The survey findings summarised in Table 9 reveal the following: moderate confidence cyberthreats identification potential (mean = 3.23, std. =0.869), passwords for online accounts were sometimes updated (mean = 3.18, std. 0.795), moderately familiar to phishing, malware, and ransomware (mean =3.36, std.0.902), Sometimes they made a backup of their important files (mean =3.68, std.0.839) and rarely reviewed the privacy settings on social media and other online accounts (mean =2.86, std = 0.834). Overall, there was an average knowledge on

cybersecurity risks seen from all variables apart from review of privacy settings (mean =2.86, std = 0.834).

Table 9: **Descriptive statistics on knowledge about cyber security risks.**

Item	N	Minimum	Maximum	Mean	Std. Deviation
*.. confidence to identify CsT	22	1	5	3.23	.869
.. often update password	22	2	5	3.18	.795
...familiarity with cyber-risks	22	1	5	3.36	.902
... back up frequency	22	2	5	3.68	.839
.. privacy settings update	22	2	4	2.86	.834

⇒ ** Questions start with wording how, and this section had 5 Likert scales.

4.6 Knowledge On cyber-Security procedures

This section aimed at gathering information regarding knowledge on cybersecurity procedures among respondents through 5 questions, that were answered based on a Likert scale 1-5 ranging from no knowledge to extremely knowledge. Questions included 1. how important you believe cyber security is to protecting sensitive information, 2.how confident in understanding of CS procedures and policies in your organization, 3.how often do you attend CS training and awareness in your organization, 4.how frequent suspicions are reported to IT department and 5. update frequency of latest software applications to own computers and mobile phones.

Findings are summarized in Table 10 below and reveal the following: Respondents believed CS awareness was very important aspect in relation to protection of sensitive information (mean = 4.68, std. 0.477), were moderately confident in understanding of CS procedures and policies at own workplaces (mean =3.78, std.0.767), sometimes they attended CS training and awareness sessions at work (mean =3.09, std. 0.921), sometimes reported

suspicious activities and security incidents to their IT department (mean 3.36, std. 1.136) and they often updated to latest software and apps (mean 4.18, std. 0.733).

Although CS is important in protection of sensitive information (mean =4.68, std. 0.477) it cannot be achieved if organizations procedures and policies are too complicated for employees to understand (mean =3.78, std. 0.767). Thus, there is still need for employee training and creation of awareness about CSR at work (mean = 3.09, std. 0.921).

Table 10**: Descriptive statistics on Knowledge about cyber security procedures.**

Item	N	Minimum	Maximum	Mean	Std. Deviation
*.. protecting sensitive information	22	4	5	4.68	.477
.. understanding policies at workplace	22	2	5	3.78	.767
...frequency and update of CS training at work	22	1	5	3.09	.921
... reporting frequency-suspicious incidents	22	1	5	3.36	1.136
.. privacy software update/patching	22	3	5	4.18	.733

* Leading questions, ... a question begins.

4.7 Knowledge On cyber-Security mitigation strategies

The aim of this section was to map respondents' knowledge level regarding cyber security mitigation strategies Two questions were raised, and responses are based on a five alternatives Likert scale (AP). Questions included how familiar you with concept of multifactor authentication and how often latest security patches are were updated.

Findings are summarised in Table 11 below and indicate the following: respondents often updated their gadgets to ensure latest security patches (mean=4, std. 0.756) although they were less familiar with mitigation procedures within their organisations (mean 2.95, std. 1.214). This observation is correlated with employees insecurity in security procedures and limited training and awareness observed in table Table 2.

Table 11**: Descriptive statistics on Knowledge about cyber security mitigation strategies**

Item	N	Minimum	Maximum	Mean	Std. Deviation

*.. Knowledge on mitigation procedures	22	1	5	2.95	1.214
.. update with latest software	22	3	5	4.00	.756

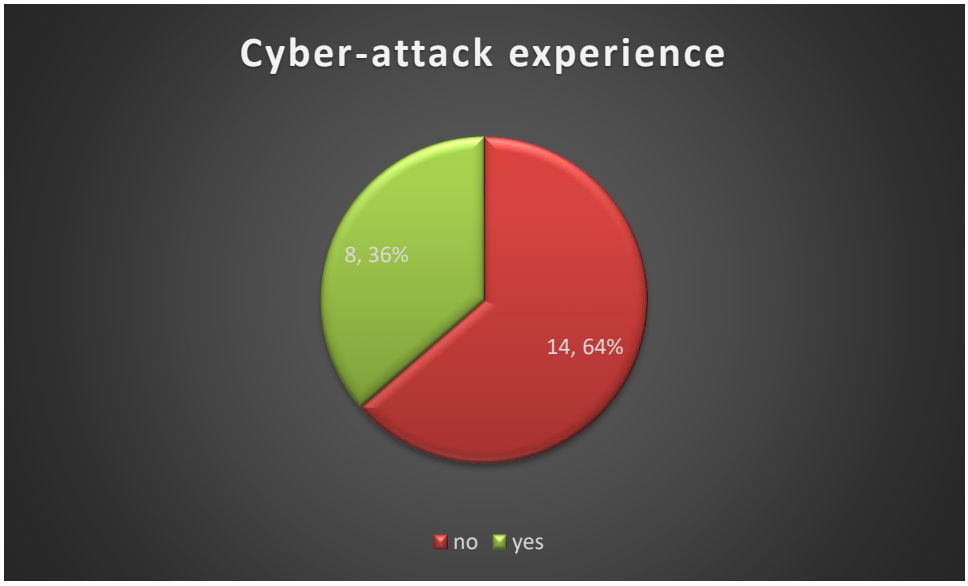
4.8 Mitigation strategies before, during and after attacks.

The aim of this section was to learn about mitigation strategies and often experienced cyber-attacks in companies and organisations. Mitigation strategies were categorised under three subsections which include: The preventive, The real time in the event of an attack and The Aftermath – those strategies undertaken after the attacks have happened. The section has the five questions with each its own sub questions. The first question seeks to find if respondents have ever experienced cyber cyber-attack, The second at knowing what type of attack, the third seeks for a rating of Preventive practices, the fourth asks about practices organisation undertake during the attacks and, fifth asks respondents to write down suggestions about own personal practices undertaken after cyber-attacks.

4.8.1 Cyber attach experience.

We wanted to find out the extent to which respondents had experienced cyber-attacks. The question required yes or no. Figure 5: Cyber-attack experience, shows the summary, whereby out of the 22 participants only 8 had experienced, which is a percentage of 36.4%. The majority 14, 64% had not experience cyber-attacks yet.

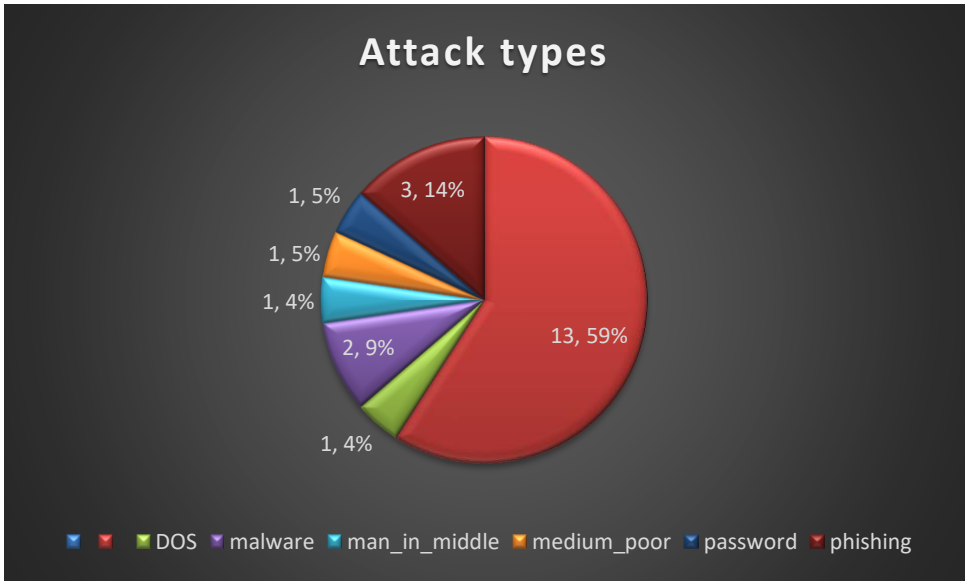
Figure 5: Cyber-attack experience



4.8.1 Cyber-attack types

Under this subsection, we wanted the respondents to tick off what type of attach they had experienced. The list of alternatives they had to choose included password attack, malware, medium poor, denial of services, man in the middle and phishing. There were 13 responses on this question, out of the 22. It was Malware and Phishing that respondents had experienced the most. Figure 6 shows 14% had experienced attacks in form of phishing, while 9% had experienced malware. The 59% never specified.

Figure 6: Experienced cyber- attack types.



N =22, N=9 usable

In a nutshell, although most respondents had not experienced cyber-attacks as seen in Figure 5, the few whom had experienced it reported phishing and malware as the mostly experienced above.

4.9 Preventive Strategies.

This subsection aims at rating the preventive strategies used by companies and individuals for cyber-security threats (CST). We thus based on often cited preventive cyber strategies in the literature for example p. 30. Based on Likert scale 1-6, where 6 is very good participants gave a rating summarised in Table 12**: Descriptive statistics on preventive mitigation strategies**. Findings show that companies were engaging several preventive measures to mitigate the likelihood of cyber threats. Companies had policies on use of personal devises (mean =5.09, std. = 0.684), engaged in cyber training and creating awareness (mean =5.05, std.=0.722), they avoided using personal devises on systems and were mostly aware of procedures to follow (mean =5.14, std.= 0.710).

Table 12**: Descriptive statistics on preventive mitigation strategies**

Item	N	Minimum	Maximum	Mean	Std. Deviation
Cyber training and awareness	22	4	6	5.05	0.722
Compliance monitoring in line with legal procedures	22	4	6	4.77	0.612
Company policy on use of personal devices	22	4	6	5.09	0.684
Specific company procedures are in accordance to required regulations	22	2	6	4.95	0.844
Not using personal devises on systems	22	3	6	5.00	0.873
Aware of the procedures to follow.	22	4	6	5.14	0.710

Source: (own construct)

4.10 Mitigation strategies during (real time) cyber-attacks.

The aim of this subsection is to map real time mitigation strategies as discussed in empirical studies page 31. The question had 5 alternatives where respondents gave their view based on a 6-point Likert scale, ranging from; 1. Very poor, 2. Poor, 3. Medium poor, 4. Fair, 5. Good and 6. Very good. The following alternatives are given; 1. shut down the system, 2. component isolation, 3. real time monitoring, 4. task force and 5. partner interaction. The findings are summarised in Table 13 the findings below.

The findings indicate that most of respondents had a specialised unit within organisations that responded cyber-attacks (mean =5.10, std.=0.889). They also isolated the components (mean =4.90, std.=0.889) while they held back information from their partners to some extent (mean =4.70, std.=1.218). Shut down was not a top priority (mean =4.71, std.=0.956)

Table 13**: Descriptive statistics on mitigation strategies undertaken during cyber-attacks.**

Item	N	Minimum	Maximum	Mean	Std. Deviation
Shutdown	22	3	6	4.71	0.956
Isolate	22	3	6	4.90	0.889
Real time monitoring	22	2	6	4.76	0.995
Task force	22	3	6	5.10	0.889
Partner interaction	22	1	6	4.70	1.218

4.11 Mitigation strategies after cyber-attack

In this subsection, respondents were requested to freely write what them and their organisations did in the aftermath of cybersecurity threats attack. As Kuhn, (2021) urgues, a collective cyber security perception and following sector guidelines is one of the practical ways through which mitigation strategies can be derived (Kuhn, Bicakci, et al., 2021). As in this case where the sample had experienced participants. Table 14: Mitigation aftermath threats is a summary of outlined actions that were freely written by experts in study. These included carrying out system security audits, technical methods- Vertical local area networks (VLANS) and procedures, they create lessons learned, task force, security diagnosis.

Table 14: Mitigation aftermath threats

Aftermath Actions		
Carry out system security audit	1	10
Cleaned, PCs and servers and added VLANs. Personal were also trained and lots of new procedures implemented.	1	9
Create lesson learned to share with the organisation	1	8
I believe that our IT dept. takes a lot of safety measures in this regard. They are being the expert in the system, they take care.	1	7
If we received a malicious email, we do not open the said email and we report immediately to our IT DEPARTMENT.	1	6
Inform it dept which will set up a task force for counter measures. Disconnect essential systems from internet	1	5
report to IT and wait for instructions	1	4

Report to shore to IT Department. They will direct us on what action to take	1	3
Update firewalls, info on awareness and ensure any software is up to date.	1	2
when reported to IT department that a phishing email was unintended opened the IT department run security/testing programs before work on the PC/station was allowed to be continued	1	1

CHAPTER FIVE: DISCUSSION OF FINDINGS

5.0 Chapter Overview

This section discusses a general evaluation of findings from the previous chapter, their meaning, importance, and value. These discussions are linked to empirical studies, industrial reports, and the research problem of which the main objective is to explorer security perception and mitigation measures. Furthermore, the section highlights on discussions' implication to the industry and other stakeholders.

5. 1 Evaluation of the findings

The survey methodology applied in this study identifies maritime cyber security perception and risk mitigation strategies, from the shipping context. The study questions were answered based on operation instrument shown on page 71. Cyber security in a maritime context as defined on page 13, in a risk exposure perspective. It is a measure of an extent to which a technology asset could be threatened by potential circumstances which may result in shipping related operational safety failures, because of information or system being corrupted, lost, or compromised (IMO,2017, p1).

5.2 Discussion on cyber- security risk perception

From the results in section 1-4;

Table **8: Descriptive statistics on knowledge about cyber security incidents**, Table 9**: Descriptive statistics on knowledge about cyber security risks.** Table 10**: Descriptive statistics on Knowledge about cyber security procedures.** Figure 4: Most familiar cyber threats, we can generalise that there is a fair risk perception. Results illustrated a fair knowledge on the familiar threats and sources 44. However, there were indications of just following procedures, other than in-depth understanding. For example, less attention on software update and lack of a general understanding of the procedures to follow in companies. These observations are similar to other scholars for example (Afenyo & Caesar, 2023; Kanwal et al., 2022; Kuhn, Bicakci, et al., 2021; Larsen & Lund, 2021; Meland et al., 2021; Park et al., 2023c).

Having an understanding on threat types can be an indication to sensitisation about the economic repercussions threats cause.

While empirical studies rank malware and phishing as mostly identified critical threat incidents (Meland et al., 2021) and (Park et al., 2023a). The same does this study as per Figure 6, as well as extending the list with data breach consequences and social engineering as per page40. Studies urge the importance of knowledge mix where human IT and OT should be in a mix. Thus vary based on employees circumstances, company procedures, education among others (Afenyo & Caesar, 2023; Larsen & Lund, 2021; Ungkap & Daengsi, 2022a). Our results also pointed to work experience, gender, and employee ranks. It seemed that the more employees stayed in the companies (15++) the less they bothered to update their knowledge or attending training sessions- A-2d. Additionally, managers are assumed to possess much more knowledge on current incidents to be able to demonstrate it to their subordinates (Afenyo & Caesar, 2023; Larsen & Lund, 2021). In this case the crew managers demonstrated a neutral understanding on cyber security which resonates with Afenyo and Caesar (2023), who advises a need for a robust human resource allocation to ensure knowledge down flow (Afenyo & Caesar, 2023). The three elements that underpin Cyber security awareness include; People, process and technology (Ungkap & Daengsi, 2022b). Several factors determine and measure cyber threat awareness such as Attitude, Cognitive, Experience in cyber-attacks, Education, and gender. The cognitive- also the people, are most important. Even though our study was dominated by respondents that had never experienced cyber-attacks, The study did not perceive high experience as relevant to cyber perception. Newcomers perceived and were more knowledgeable to cyber threats, neither did education count however some indications may point to gender difference. We also identified some threats in line with Park et, (2019). These were the four cyberthreats connections, lack of training and expertise, use of outdated IT systems, Hacktivism and fake site and phishing.

The outdated systems are a main cause of threats that necessitates clear organisational procedures to be understood as in the case of NIST where industries are generally advised. Unlike scholars, pointing at sluggishness regarding vulnerabilities identification in the maritime for example McNicholas (2016), we observe tendencies in the pipeline as it seems there is a fair awareness level based on our research findings. These findings are also in direction of research concerned with, a huge global impact related to cyber Security in maritime, where sensitization in different contexts is a crucial step (DNV, 2023; Kavallieratos et al., 2020; McNicholas, 2016; OECD, 2022; Park et al., 2023c; Townsend, 2022; Tusher et al., 2022a, 2022a). The attack surface is getting more complex given technological advancements that are

said to head from industry 4.0 and 5.0. Yet in some cases the OT may seem less aligned to IT. This is what our findings also see, when crew managers bear less knowledge on CT, yet need to use OT to reach out to the onshore personnel.

5.3 Discussion on Mitigation Procedures

Regarding the mitigation strategies, findings show various procedures were undertaken Table 12**: Descriptive statistics on preventive mitigation strategies**. Most companies focused on precautionary, while few were on real time, and aftermath. A similar observation was undertaken by Cheung & Bell (2021) , a problem linked to over reliance on aftermath and precautionary can be that security procedures can be lagging behind, given the speed of attack tactics (Cheung & Bell, 2021). A global technology innovator IBM (2023) resonates with empirical studies on mitigation when they say.

> Attackers have different tactics, and they keep changing. However, they are mostly taking advantages of loose doors. For example, in 2023, 21% of incidents were backdoors deployed, 17% in 22 were ransomware and 6% of attacks were business email compromise (IBM, 2023, pp. 3–4).

This shows a need not only to understanding the threat type, but also know its behaviour and how it comes about. This necessitates a balanced framework such as NIST

Although findings indicated over reliance on precautionary strategies, at the same time some preventive measures performance varied. While training and awareness took more focuss 47, and in line with the literature (Afenyo & Caesar, 2023; Kanwal et al., 2022; Meland et al., 2021; Park et al., 2023c), that acknowledge its importance towards threats and a need for thorough crew training. The training should consider the dynamic threat environments. The legal environment seems to be a challenge in our study findings, which is in line with the literature for example (Afenyo & Caesar, 2023; Kanwal et al., 2022; Weaver et al., 2022), which poses a challenge to relevant training. In their European funded research article MITIGATE, Duzha et al, (2017) identify collaboration as very important, which can enrich knowledge across (Duzha et al., 2017). The objective of MITIGATE is to realise a radical shift in risk management methodologies for maritime sector towards a collaborative evidence-based method that alleviates limitation in risk management frameworks. In this study a clear limitation to most of the respondents was legal framework and complicated procedures. MITIGATE emphasise collaboration of various stakeholders, in areas; Identification, Assessment and

Mitigation of risks associated with cyber assets. The industrial standards for example, some companies seemed to a certain to adopt DNV`s[7] four recommended steps.

The industry nevertheless demonstrates efforts. Various bodies; classification societies, organisations and unions have developed individual guidelines for the protection of (CI) against cyberthreats (ABS, 2016; BIMCO, et al., 2017; DNVGL, 2016). For example BIMCO `s guidelines for ship board IT and OT systems for threat identification and vulnerabilities, their assessment, development of mitigation and contingency measures, and responding and recovering from such threats (BIMCO, et al., 2017). American bureau of shipping`s (ABS), guidelines for marine and offshore on CS , best practices, criteria for system assessment, concepts of data Integrity, software system Verification and Quality management (ABS, 2023). The classification societies,(DNV, 2023; DNVGL, 2016; Lloyd`s Register, n.d.) do guide stakeholders on technology implication, the implementation and design, as well as standard application such as ISO/IEC27001 and ISA-99/IEC-62443-applicable to OT security for control systems for critical assets industrial assets. These initiatives do mirror an offensive perception.

In addition, it resonates with increasing efforts in sensitization and update in new security frameworks for critical infrastructures annually. For example, in addition to other industrial updates, on a general note the NIST cyber security framework that has long existed is now being updated to CSF 2.0 (BIMCO, 2019; DNV, 2023; NIST, 2022). NIST has an aim to address the current and future CS risks and to make it easier for all organisations to adopt. The challenge to organisations is to align safety culture in daily operations – an issue by ISM and ISPS 2.3 Cybersecurity Perception. Even though procedures are perceived to be in place, it raises an alarm when few understand how they are being practiced. However, as other studies still indicated (Afenyo & Caesar, 2023; Ungkap & Daengsi, 2022), imparting the knowledge can be challenging, the training and school curriculars and policies at times seem not aligned which is in line with this study too. Therefore, NIST centres on a wide collaboration when they recommend a step by step 5 framework on which threat profiles can be built. In the European funded study, Ransom risk management (Barker et al., 2022, pp. 16–20), the building of a ransom profile based on NIST CFS´s Identify, Protect, Detect, Respond and Recover resonates with the fact that collaboration where knowledge can be shared will create mutual benefits. The

[7] https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/ism-guidance.html

DNV`s simplified framework for Maritime built as well on NIST CSF, sees it material to Plan, Do, Check and Act.

5.4. Summary of the combination of two main question.

In general, the main issues regarding cybersecurity perception and the mitigation procedures can be linked to ongoing literature studies whereby in the case of perception, it should not only be left to the IT departments, but rather to combine the human behaviour as well. There is vast evidence that human behaviour although a vital resource, can also have linkage to cyber threats. Therefore, training and procedures that incorporate the human behaviour with interaction of IT /OT can be considered vital step towards developing more appropriate mitigation strategies that balance the 3 levels.

5.5 Discussions on implication of research to Maritime stakeholders

Cyber- security threats within maritime industry are continuously on a free foot considering recently re-occurring threats. For example (Garry, 2023; Kovacs, 2020; Kuhn, Bicakci, et al., 2021; Seatrade, 2023). It is also a focus to corporations and organisations worldwide for example (GCE, 2023; WEF, 2023), and is exacerbated by emerging technologies (Larsen & Lund, 2021; Park et al., 2023c; Tusher et al., 2022a). Our study has a similar direction, that this area needs constant attention from scholars. Reliance on novel technologies in the maritime and in other organisations and corporations will increase and thus a reflection on steps forward is needed.

Cybersecurity is undoubtedly a major vulnerability, and our study has also mirrored a similar perception. To minimise the vulnerability studies are suggesting a diversity of frameworks and standards. For example, 24. The NIST framework is widely used as a basis to ease on the rigorous risk architectures (Barker et al., 2022), Various industrial risk mitigation profiles adapt their works on NIST for example IMO 25 and DNV cyber security guidelines 13. In all the five steps; (Identify, Protect, Detect, Respond and Recover) (NIST, 2022) collaboration in mitigation is essential (Duzha et al., 2017). Where there is collaboration, on each stage of the risk analysis, it increases knowledge sharing across, which is a necessity to the industry. There is need to understand the necessity looking at OT and IT beyond a field for only IT managers, but also a general human resource in organisations where everyone has a stake, if cyber insurgency is to be tackled.

In our study we identified more tendencies towards preventive strategies but at the same time tendencies of leaving matters to special task forces. Although it is a good practice having special units within organisations that tackle security issues, the procedures should be clearer

to the entire personnel and on continuous basis. The maritime industry could lobby for a revision of internal procures in companies, which in this case already exist through the ISM code and IMO resolution [4]. However, interpretation is left to managers which still is a challenge which may mean – simply to tick off as a way of fulfilling compliance. As scholarly articles were concerned about knowledge and school curriculum (Afenyo & Caesar, 2023; Kanwal et al., 2022), it is likely that those that with longer experience necessary did not illustrate a better understanding in cyber prevention initiatives. There seem to be indications that school curriculums need to be reviewed whereby irrespective of age, culture the understanding of security should be uniform. It could also be an indication that freshers from universities can start right away on managerial levels in cybersecurity tasks. The maritime community and other stakeholders can gain advantage if they build collaborating teams with different backgrounds who act in real time. The collaboration will boost transparency in risk handling by various stakeholders while at the same time will generate unique evidence about risk assessment and mitigation.

The managers ought to share cyber security knowledge across the organisation and all employees in a simple language preferably in form of a continuous loop. To ease this undoubtedly challenging task, The classification societies worked out relevant guidelines for safety management systems to OT and IT (DNV, 2023; DNVGL, 2016; Lloyd`s Register, n.d.). They are meant to guide stakeholders on technology implication, the implementation and design, as well as standard application such as ISO/IEC27001 and ISA-99/IEC-62443. These guidelines ; Plan, Do, check and Act (DNV, 2023; Kuhn, Bicakci, et al., 2021) break down the task as explained below.

The Planning stage is where a solid foundation takes place. It stars with identification of cyber security objectives that are relevant for safe operations of OT/IT system. The IMO`s requirements and those of external and internal stakeholders are part of the objectives. The defined objectives guide in the generation of inventory of safety and critical systems and software, which are necessary in execution of cyber risk assessment. A through assessment is in four levels according to DNV (2023). 1) Consequential analysis in terms of loss of Confidentiality, Integrity, and Availability for each, 2) Probability analysis on how often a particular system can be compromised, 3) Ranking based on OT/IT vulnerability and 4) Determination of required barriers- in terms of people, processes, and technology to combat the risk.

At the next stage – DO, the results in the previous stage should be utilised to define an implementation plan for rolling out suitable mitigators. As a minimum DNV recommends

several functional requirements for a safety management system: A security policy, Instructions, and procedures to ensure a safe cyber operation, Defined authority levels and communication policy among entire personnel, Reporting procedures of the attack, Procedure to prepare for and respond towards the attack, and prepare for internal cyber audits and management review. Furthermore, is training for different levels bearing in mind the interconnections of Process, technology and people which is in line with several scholars that identify the necessity of crew training towards threat prevention for example (Afenyo & Caesar, 2023; DNV, 2023; Meland et al., 2021).

The checking process must then be continual and include the evaluation of the effectiveness of achieving security objective, analysis of cyber events and reports, evaluation of logs and intrusion detection systems, and the external checks to evaluate the environment generally. After findings are reviewed, then corrections and other course actions can be put in pipeline. A key to future successful cyber resilience requires a constant update of cyber risk assessment, policies and procedures as described, due to a non-static environment. The checking process Lastly preventive actions will then be implemented based on the findings of internal and external review reports.

Whereas studies on maritime cybersecurity are underway, those that combine a general understanding in the perspective of capturing the perception of maritime personnel and the mitigation strategies combined are few. In this angel our thesis has a unique contribution.

5.6 The study Limitations

Factors relevant to perceptions and mitigation are being studied and linked to several theories. This study has taken a more explorative nature in contributing to existing research by reaching industrial experts and therefore findings are not hooked to theories. It is however worth mentioning that generalization of the study findings must be done with caution given some discussions below.

Even though our sample was purposive, whereby respondents were from maritime related environments as shown in Table 6: Company and organisation types, the size was rather small as illustrated Table 7**: Overview of respondents**. With such a limitation in the studies Sample size findings may need scholarly backups rather than nakedly considered. Furthermore, the fact that most participants were in top management positions, and less in the seafarer lower positions, also may limit on the real problems associated with cyber security in relation to managers and personnel. On the other hand, the first-hand information from experts supplements the empirical studies, which often based on entirely systematic literature reviews. Larsen & Lund (2021) sees the need for combinations as a way of building on extensive theories

in explaining cyber risk perception (Larsen & Lund, 2021). Risk perception is a subjective cognitive process, and the dimensions can vary from population to population and contexts. Whereas this does not imply a weakness in review studies, but often throwing a glance on the realities enriches the literature, of which this study brings forward and, in this case, adding a value.

More still, a greatest percentage of our sample did not have real experience in cyber-attacks. On the other side, the fact that were experts and highly educated, may resonate with the fact that they took cautions. The study should have got participants that had experienced these problems. But since most respondents were from Norway and other OECD member countries, here they are not very many seafarers 'origins. Thus, limiting concluding based on seafarer how they perceive cyber threats.

CHAPTER SIX: CONCLUSION

6.0 Chapter Overview

The study aimed at exploring security perception and mitigation measures with Maritime shipping. To guide the study, two main research questions as identified were basis for findings and discussions already concluded in previous chapters.

We kicked off this study with an intense scholarly review see- 17 to understand the threat environment in generals. We proceeded to a more in-depth analysis of the literature review by use of visualisation software. After gaining a deeper insight the two questions that were considered suitable towards gaining an understanding on security perception and mitigation measures in the maritime shipping included: Q1 How is cyber risk perceived among seafarers and managers in the maritime Q2 What major measures are taken to mitigate cyber-risks.

6.1 Conclusion of the main findings

Regarding the first question-, we analysed responses on the four-section questionnaire on page 40 and found following main issues for our consideration.

The knowledge level was moderate, especially more aware on data breach and suspicious emails as possible cyberthreat avenues. However, the potential to identify cyberthreats seemed to continuously pose challenges which can be linked to the fact that private settings update needs more focus. Despite these instances, the culture of reporting in case of incidents was being practised to a certain degree, although understanding what and when to report is unclear, reason being complicated procedures that was not easy to understand and thus only trusted IT. With this in consideration, there seems generally a fair-risk perception. Our

basis to this conclusion is the first 4 questions However, the sample size may limit generalising these findings and results to seafarers and managers. Nevertheless, some factors are worth pointing out, even though some may seem out of this study scope, they are of interest to focus on as a way of enhancing a cyber- resilient future overall. Training and knowledge share across: There is still need for a training and knowledge that is collaborative and across teams. While many did understand the dangers associated with cyberthreats, the actual procedures were not clear and in some cases were left only to the hands of security personnel, and thus saw no need of in-depth understanding.

Regarding the second question, we found that more focus was on preventive measures compared to measures after and during the threat. This seem to be ongoing concern in the current literature too.

6.2 Future research Recommendations

In the process of exploring the perceptions and mitigation strategies, we found some interesting directions in our data that can be interesting to consider for further research. The Gender differences in maritime and their knowledge to cyber threats can give interesting perspective. There was an indication of whether women were more risk averse and therefore less prone to cyber threats compared to men. A future study can build on and to find why and what in this direction.

Another study possibility can be linked on experience and position towards security perception and mitigation. There was a tendency – although out of our study scope; that number of years and experience did correlate to knowledge and awareness in cyber security. Could it possible that the young and less experienced are more vigilant on these issues? Why is it so and what should be done?

Further consideration is to study the knowledge level of human resource personnel in relation to cyberthreats to find out if companies are making improvement efforts.

Reference list

2022: Shipping's half year report | Clarksons. (2023). https://www.clarksons.com/home/news-and-insights/2022/2022-shippings-half-year-report/

ABS. (2016). *GUIDANCE NOTES ON:The Application of Cybersecurity Principles to Marine and Offshore Operations* (pp. 1–49). https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cybersecurity_GN_e.pdf

ABS. (2023). *American Bureau of Shipping (ABS) Eagle.org*. https://ww2.eagle.org/en.htmlhttps://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cybersecurity_GN_e.pdf

Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. *Ocean and Coastal Management, 236*. Scopus. https://doi.org/10.1016/j.ocecoaman.2023.106493

Alshahrani, H. M., Alotaibi, S. S., Ansari, M. T. J., Asiri, M. M., Agrawal, A., Khan, R. A., Mohsen, H., & Hilal, A. M. (2022). Analysis and Ranking of IT Risk Factors Using

Fuzzy TOPSIS-Based Approach. *Applied Sciences (Switzerland)*, *12*(12). Scopus. https://doi.org/10.3390/app12125911

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation. *Journal of Marine Science and Engineering*, *8*(10), Article 10. https://doi.org/10.3390/jmse8100776

Androjna, A., & Perkovič, M. (2021). Impact of spoofing of navigation systems on maritime situational awareness. *Transactions on Maritime Science*, *10*(2), 361–373. Scopus. https://doi.org/10.7225/toms.v10.n02.w08

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2022). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems*, 1–14. https://doi.org/10.1109/TITS.2022.3164678

Barber, D., Kanth, V., & Rogers, D. (2022). Manipulating the Automatic Identification System with Extremely Low-Cost Hardware. *Proc IEEE Mil Commun Conf MILCOM*, *2022-November*, 541–546. Scopus. https://doi.org/10.1109/MILCOM55135.2022.10017874

Barker, W., Fisher, W., Scarfone, K., & Souppaya, M. (2022). *Ransomware Risk Management: A Cybersecurity Framework Profile* (NIST Internal or Interagency Report (NISTIR) 8374). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8374

Becmeur, T., Boudvin, X., Brosset, D., Héno, G., Merien, T., Jacq, O., Kermarrec, Y., & Sultan, B. (2017). A Platform for Raising Awareness on Cyber Security in a Maritime Context. *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, 103–108. https://doi.org/10.1109/CSCI.2017.17

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), Article 1. https://doi.org/10.3390/info13010022

BIMCO. (2019). *Cyber Security Clause 2019*. https://www.bimco.org/contracts-and-clauses/bimco-clauses/current/cyber-security-clause-2019

BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, & OCIMF and IUMI. (2017). *THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS*. https://www.maritimeglobalsecurity.org/media/1014/c-users-jpl-onedrive-bimco-desktop-guidelines_on_cyber_security_onboard_ships_version_2-0_july2017.pdf

Burrell, D., Bhargava, N., Bradley-Swanson, O., Harmon, M., Wright, J., Springs, D., & Dawson, M. (2020). Supply Chain and Logistics Management and an Open Door Policy Concerning Cyber Security Introduction. *International Journal of Management and Sustainability*, *9*, 1–10. https://doi.org/10.18488/journal.11.2020.91.1.10

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*, *42*(8), 1643–1669. https://doi.org/10.1111/risa.13687

Carnival. (2023). *Carnival Corporation Reports Ransomware Attack Accessed Data*. The Maritime Executive. https://maritime-executive.com/article/carnival-corporation-reports-ransomware-attack-accessed-data

Chang, C. H., Wenming, S., Wei, Z., Changki, P., & Kontovas, C. A. (2019). Evaluating cybersecurity risks in the maritime industry: A literature review. *Proceedings of the International Association of Maritime Universities (IAMU) Conference*.

Cheung, K.-F., & Bell, M. G. H. (2021). Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study.

European Journal of Operational Research, *291*(2), 471–481. https://doi.org/10.1016/j.ejor.2019.10.019

Cheung, K.-F., Bell, M. G. H., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*, 102217. https://doi.org/10.1016/j.tre.2020.102217

Cichen. (2020, September 28). *CMA CGM confirms ransomware attack*. Lloyd's List. https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack

Clarksons. (2021, January 8). 2020 Review: Managing Disruption & Going Green. *Clarksons Research*. https://clarksonsresearch.wordpress.com/2021/01/08/2020-review-managing-disruption-going-green/

CMA: Cyber risks raised by ongoing 'cyber war'. (2022, March 31). Seatrade Maritime. https://www.seatrade-maritime.com/cyber-security/cma-cyber-risks-raised-ongoing-cyber-war

CMACGM. (2020). *The CMA CGM group, hit by a cyberattack*. https://www.cmacgm-group.com/en/news-media/global-it-update-09-29-2020

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches.* SAGE.

Dan Craigen, Nadia Diakun-Thibault, & Randy Purse. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10). http://timreview.ca/article/835

de Peralta, F. A., Watson, M. D., Bays, R. M., Boles, J. R., & Powers, F. E. (2021). Cybersecurity resiliency of marine renewable energy systems Part 2: Cybersecurity best practices and risk management. *Marine Technology Society Journal*, *55*(2), 104–116.

DNV. (2022). *Cyber security for the real world*. DNV. https://www.dnv.com/Default

DNV. (2023). *Preparing for IMO's ISM Cyber Security*. DNV. https://www.dnv.com/Default

DNVGL. (2016). *Cyber security resilience management for ships and mobile offshore units in operation* (DNVGL-RP-0496; pp. 1–86). https://www.gard.no/Content/21865536/DNVGL-RP-0496.pdf

Donaldson, S. E., Siegel, S., Williams, C. K., & Aslam, A. (2015). *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats* (1st ed. 2015.). Apress : Imprint: Apress.

Duzha, A., Gouvas, P., & Canepa, M. (2017). MITIGATE: An Innovative Cyber-Security Maritime Supply Chain Risk Management System. *ITASEC*, 248–252.

Eck, N. van, & Waltman, L. (2009). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, *84*(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

Enayaty-Ahangar, F., Albert, L. A., & DuBois, E. (2021a). A survey of optimization models and methods for cyberinfrastructure security. *IISE Transactions*, *53*(2), 182–198. https://doi.org/10.1080/24725854.2020.1781306

Enayaty-Ahangar, F., Albert, L. A., & DuBois, E. (2021b). A survey of optimization models and methods for cyberinfrastructure security. *IISE Transactions*, *53*(2), 182–198. https://doi.org/10.1080/24725854.2020.1781306

Eurostat. (2023). *Glossary:Enterprise size*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Enterprise_size

Frankfort-Nachmias, C., Nachmias, D., & DeWard, J. (2015). *Research methods in the social sciences* (8th ed.). Worth publishers.

Freeze, D. (2020, November 10). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine*. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Garry. (2023, January 19). *DNV ransomware attack 'concerning': Cyber Threat Analyst*. Seatrade Maritime. https://www.seatrade-maritime.com/cyber-security/dnv-ransomware-attack-concerning-cyber-threat-analyst

GCE. (2023). *Sørlandets Energikonferanse 2023*. GCE NODE. https://gcenode.no/event/sorlandets-energikonferanse-2023/

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. *Wired, August, 22*.

IBM. (2023). *IBM Security X-Force Threat Intelligence Index 2023* (pp. 1–58). https://www.ibm.com/reports/threat-intelligence

ICS. (2023). *International Chamber of Shipping*. https://www.ics-shipping.org/

IMO. (2017a). *GUIDELINES ON MARITIME CYBER RISK MANAGEMENT MSC-FAL.1/Circ.3 5 July 2017* (pp. 1–4) [ANNEX GUIDELINES ON MARITIME CYBER RISK MANAGEMENT]. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

IMO. (2017b). *MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS* (p. 1). https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

IMO. (2022). *Maritime cyber risk*. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-

%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

IMO-ISPS. (2021). *Guide to Maritime Security and the ISPS Code (2021 Edition)*. Witherbys. https://shop.witherbys.com/guide-to-maritime-security-and-the-isps-code-2021-edition/

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., & Chang, C.-H. (2022). Maritime cybersecurity: Are onboard systems ready? *Maritime Policy & Management*, *0*(0), 1–19. https://doi.org/10.1080/03088839.2022.2124464

Kapalidis, C., Karamperidis, S., Watson, T., & Koligiannis, G. (2022). A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships. *Journal of Marine Science and Engineering*, *10*(10). Scopus. https://doi.org/10.3390/jmse10101486

Karim, M. S. (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? *Marine Policy*, *143*. Scopus. https://doi.org/10.1016/j.marpol.2022.105138

Kavallieratos, G., Diamantopoulou, V., & Katsikas, S. K. (2020). Shipping 4.0: Security Requirements for the Cyber-Enabled Ship. *IEEE Transactions on Industrial Informatics*, *16*(10), 6617–6625. https://doi.org/10.1109/TII.2020.2976840

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, *37*. Scopus. https://doi.org/10.1016/j.ijcip.2022.100526

Kovacs, E. (2020, October 6). *UN Maritime Agency Hit by 'Sophisticated Cyberattack'*. SecurityWeek. https://www.securityweek.com/un-maritime-agency-hit-sophisticated-cyberattack/

Kuhn, K., Bicakci, S., & Shaikh, S. A. (2021). COVID-19 digitization in maritime: Understanding cyber risks. *WMU Journal of Maritime Affairs*, *20*(2), 193–214. https://doi.org/10.1007/s13437-021-00235-1

Kuhn, K., Kipkech, J., & Shaikh, S. A. (2021). Maritime ports and cybersecurity. In *ICT Solutions and Digitalisation in Ports and Shipping* (pp. 37–68). Institution of Engineering and Technology; Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85115721619&partnerID=40&md5=514f2b4b292e636e3837813398d654e2

Larsen, M. H., & Lund, M. S. (2021). A Maritime Perspective on Cyber Risk Perception: A Systematic Literature Review. *IEEE Access*. Scopus. https://doi.org/10.1109/ACCESS.2021.3122433

Lloyd`s Register. (n.d.). *Shipping needs to raise its cyber game.* Lloyd's Register. Retrieved 23 March 2023, from https://www.lr.org/en/insights/articles/shipping-needs-to-raise-its-cyber-game/

Maritime Executive. (2023). *Saipem's Servers Hit by Cyberattack*. The Maritime Executive. https://maritime-executive.com/article/saipem-s-servers-hit-by-cyberattack

Maritime safety committe. (2017). *MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS*. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

Marr, B. (n.d.). *Cyber Apocalypse 2023: Is The World Heading For A 'Catastrophic' Event?* Forbes. Retrieved 1 March 2023, from https://www.forbes.com/sites/bernardmarr/2023/02/06/cyber-apocalypse-2023-is-the-world-heading-for-a-catastrophic-event/

McNicholas, M. (2016). *Maritime Security: An Introduction*. Butterworth-Heinemann.

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*.

Meland, P. H., Nesheim, D. A., Bernsmed, K., & Sindre, G. (2022). Assessing cyber threats for storyless systems. *Journal of Information Security and Applications*, *64*. Scopus. https://doi.org/10.1016/j.jisa.2021.103050

Munim, Z. H., Dushenko, M., Jimenez, V. J., Shakil, M. H., & Imset, M. (2020). Big data and artificial intelligence in the maritime industry: A bibliometric review and future research directions. *Maritime Policy & Management*, *47*(5), 577–597. https://doi.org/10.1080/03088839.2020.1788731

Munim, Z. H., & Schramm, H.-J. (2018). The impacts of port infrastructure and logistics performance on economic growth: The mediating role of seaborne trade. *Journal of Shipping and Trade*, *3*(1), 1. https://doi.org/10.1186/s41072-018-0027-0

NIST. (2022). Updating the NIST Cybersecurity Framework – Journey To CSF 2.0. *NIST*. https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

OECD. (2021). *Ocean shipping and shipbuilding—OECD*. https://www.oecd.org/ocean/topics/ocean-shipping/

OECD. (2022). *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity | READ online*. Oecd-Ilibrary.Org. https://www.oecd-ilibrary.org/docserver/a69df866-en.pdf?expires=1676568607&id=id&accname=guest&checksum=39CF2B6AC0813DB64326F213772FE25E

Oruc, A., Amro, A., & Gkioulos, V. (2022). Assessing Cyber Risks of an INS Using the MITRE ATT&CK Framework. *Sensors*, *22*(22), Article 22. https://doi.org/10.3390/s22228745

Park, C., Kontovas, C., Yang, Z., & Chang, C.-H. (2023a). A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean and Coastal Management*, *235*. Scopus. https://doi.org/10.1016/j.ocecoaman.2023.106480

Park, C., Kontovas, C., Yang, Z., & Chang, C.-H. (2023b). A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management*, *235*, 106480. https://doi.org/10.1016/j.ocecoaman.2023.106480

Park, C., Kontovas, C., Yang, Z., & Chang, C.-H. (2023c). A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management*, *235*, 106480. https://doi.org/10.1016/j.ocecoaman.2023.106480

Park, C., Shi, W., Zhang, W., Kontovas, C., & Chang, C.-H. (2019a). Cybersecurity in the maritime industry: A literature review. In Svilicic B., Mori Y., & Matsuzaki S. (Eds.), *Commem. Annu. Gen. Assem., AGA - Proc. Int. Assoc. Marit. Univ. Conf., IAMUC* (pp. 79–86). International Association of Maritime Universities; Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85078043331&partnerID=40&md5=b83f8598f9863c63990cad3c692ca702

Park, C., Shi, W., Zhang, W., Kontovas, C., & Chang, C.-H. (2019b). *Cybersecurity in the maritime industry: A literature review*. 79–86. Scopus.

Rahman, S., Hossain, N. U. I., Govindan, K., Nur, F., & Bappy, M. (2021). Assessing cyber resilience of additive manufacturing supply chain leveraging data fusion technique: A model to generate cyber resilience index of a supply chain. *CIRP Journal of Manufacturing Science and Technology*, *35*, 911–928. https://doi.org/10.1016/j.cirpj.2021.09.008

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., & Harnisch, M. (2015). Industry 4.0: The future of productivity and growth in manufacturing industries. *Boston Consulting Group*, *9*(1), 54–89.

Seatrade. (2023, January 19). *DNV ransomware attack 'concerning': Cyber Threat Analyst*. Seatrade Maritime. https://www.seatrade-maritime.com/cyber-security/dnv-ransomware-attack-concerning-cyber-threat-analyst

Sekaran, U., & Bougie, R. (2019). *Research Methods For Business: A Skill Building Approach*. John Wiley & Sons.

Shen. (2018, July 25). *Cosco Shipping targeted in ransomware attack*. Lloyd's List. https://lloydslist.maritimeintelligence.informa.com/LL1123581/Cosco-Shipping-targeted-in-ransomware-attack

Shippingwatch. (2021, September 20). *CMA CGM hit by new cyberattack*. https://shippingwatch.com/carriers/https%3A%2F%2Fshippingwatch.com%2Fcarriers%2Farticle13295440.ece

Stopford, M. (2008). *Maritime Economics 3e*. Routledge.

Techcrunch. (2023, February 21). Phishing. *TechCrunch*. https://techcrunch.com/tag/phishing/

Thomas, M. L. (2022). Maritime Hacking Using Land-Based Skills. In Jancarkova T., Visky G., & Winther I. (Eds.), *Int. Conf. Cyber Confl., CYCON* (Vols 2022-May, pp. 249–263). NATO CCD COE Publications; Scopus. https://doi.org/10.23919/CyCon55549.2022.9811049

Townsend, K. (2022, May 18). *The Vulnerable Maritime Supply Chain—A Threat to the Global Economy*. SecurityWeek. https://www.securityweek.com/vulnerable-maritime-supply-chain-threat-global-economy/

Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T.-E., & Nazir, S. (2022a). Cyber security risk assessment in autonomous shipping. *Maritime Economics & Logistics*, *24*(2), 208–227. https://doi.org/10.1057/s41278-022-00214-0

Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T.-E., & Nazir, S. (2022b). Cyber security risk assessment in autonomous shipping. *Maritime Economics and Logistics*, *24*(2), 208–227. Scopus. https://doi.org/10.1057/s41278-022-00214-0

UIO. (2023). *Nettskjema*. https://nettskjema.no/user/form

UNCTAD. (2020a). *COVID-19 and maritime transport: Impact and responses*. 77.

UNCTAD. (2022). *REVIEW OF MARITIME TRANSPORT 2021*. UNITED NATIONS.

UNCTAD. (2023). *Review of maritime Sector- 2020* (pp. 1–159). https://unctad.org/system/files/official-document/rmt2020_en.pdf

UNCTAD. (2020b). *Merchant fleet*. UNCTAD E-Handbook of Statistics 2020. https://stats.unctad.org/handbook/MaritimeTransport/MerchantFleet.html

Ungkap, P., & Daengsi, T. (2022a). Cybersecurity Awareness Modeling Associated with Influential Factors Using AHP Technique: A Case of Railway Organizations in Thailand. *2022 International Conference on Decision Aid Sciences and Applications (DASA)*, 1359–1362. https://doi.org/10.1109/DASA54658.2022.9765092

Ungkap, P., & Daengsi, T. (2022b). *Cybersecurity Awareness Modeling Associated with Influential Factors Using AHP Technique: A Case of Railway Organizations in Thailand*. 1359–1362. Scopus. https://doi.org/10.1109/DASA54658.2022.9765092

Waltman, L., & van Eck, N. J. (2012). A new methodology for constructing a publication-level classification system of science. *Journal of the American Society for Information Science and Technology*, *63*(12), 2378–2392. https://doi.org/10.1002/asi.22748

Weaver, G. A., Feddersen, B., Marla, L., Wei, D., Rose, A., & Van Moer, M. (2022). Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach. *Transportation Research Part C: Emerging Technologies*, *137*. Scopus. https://doi.org/10.1016/j.trc.2021.103423

WEF. (2023, January 18). *Press Conference: Global Cybersecurity Outlook 2023*. World Economic Forum. https://www.weforum.org/events/world-economic-forum-annual-meeting-2023/sessions/press-conference-global-cybersecurity-outlook-2023/

Wei Zhe. (2017, October 16). *BW Group computers hit by cyber attack in July*. Lloyd's List. https://lloydslist.maritimeintelligence.informa.com/LL111889/BW-Group-computers-hit-by-cyber-attack-in-July

Appendices

Appendix 1: A) Survey questionnaire

MARITIME CYBER SECURITY MITIGATION

Dear Participants!

My name is Valerie-Peggy I Korsvik. A University of South–Eastern Norway USN student, Faculty of Technology, Natural Sciences and Maritime Sciences. I am working on my master's thesis - Cyber-security risk and Mitigation Strategies Perception within the Maritime, for which I kindly request your participation in this survey.

Cybercrime is recognized as one of the most significant threats any company will face in the following decades. The introduction of automation, integration, and the drive to digitalize systems and processes makes companies prone to cyber threats. This trend is on high-speed in the maritime sector.

We base on review studies to adopt a three-stage approach for maritime stakeholders to enhance security.

1. Precautionary measures: Involves defensive action plans implemented before the occurrence of a cyberattack.

2. Real-time recovery measures: Defensive action plans implemented during a cyberattack.

3. Aftermath Measures: Action plans that are implemented after a cyberattack

This questionnaire explores security perceptions and mitigation measures undertaken before, during, and after the attack.

The survey is estimated to take 10-15 minutes of your precious time.

The instrument includes a 5-point Likert scale, where items are scored (measured) from 1 to 5, and others are rated in wordings. The items describe various aspects. Therefore, you are requested to indicate to which extent you agree or disagree or rating of good, to not good with the item by ticking the number or selecting the word that reflects your opinion(s).

Your participation is voluntary, and the information you share, and your identity will be held strictly confidential. My supervisor Associate Minim from USN, approved this questionnaire, and there is no risk associated with the study.

Thank you for participating in our survey. We also appreciate it If you know of others interested in this study to pass this questionnaire on to them. Please do not hesitate to contact us in the emails below in case of any queries.

Kind regards,

Master student: Valerie- Peggy I Korsvik

Email: 231167@usn.no; v.korsvik@gmx.com

Supervisors: Associate professor Ziaul Haque Munim, Faculty of Technology, Natural Sciences and Maritime Sciences, Institute for maritime operations Campus – Vestfold (D3-52) Ziaul.H.Munim@usn.no

31 00 86 89 / 998 93 486

b)

SECTION A: BACKGROUND INFORMATION

1. Company/organization type:

Select …

2. Work experience

- ○ 0-5 years
- ○ 6-10 years
- ○ 11-15 years
- ○ 15+ years

3. Location

Select …

4. Write location here if not on list above

5. Sex of Respondent

- ○ Male
- ○ Female
- ○ Other

6. Your position

Select …

7. Highest Level of education attained by respondent

- ○ High School
- ○ Graduate degree
- ○ masters degree
- ○ Phd/ doctoral

c)

SECTION B: KNOWLEDGE ON CYBER SECURITY INCIDENTS

8. Items on cyber security incidents:

	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
I am familiar with malware attacks	○	○	○	○	○
I have adequate knowledge on phishing	○	○	○	○	○
I am aware of social engineering	○	○	○	○	○
I understand the potential consequences of data breaches	○	○	○	○	○
I know how to recognize suspicious emails	○	○	○	○	○
I have knowledge on how to avoid fake websites	○	○	○	○	○
I can recognize unsecured networks	○	○	○	○	○

d)

SECTION C: KNOWLEDGE ON CYBER SECURITY RISKS

10. How confident do you feel in identifying potential cybersecurity threats?

Select ...

11. How often do you update your passwords for your online accounts?

Select ...

12. How familiar are you with common cyber security risks such as phishing, malware, and ransomware?

Select ...

13. How often do you back up your important files and data?

- ○ 1. Never
- ○ 2. Rarely
- ○ 3. Sometimes
- ○ 4. Often
- ○ 5. Always

14. How frequently do you review your privacy settings on social media and other online accounts?

Select ...

e)

SECTION D: KNOWLEDGE ON CYBER SECURITY PROCEDURES

15. How important do you believe cyber security is to protecting sensitive information?

Select …

16. How confident are you in your understanding of the cyber security procedures and policies in place at your organization?

Select …

17. How often do you attend cyber security training or awareness sessions?

Select …

18. How frequently do you report suspicious activity or security incidents to your IT department?

Select …

19. How often do you update software and applications on your computer or mobile device to ensure they are protected against the latest security threats?

Select …

f)

SECTION E: KNOWLEDGE ON CYBER SECURITY MITIGATION STRATEGIES

20. How familiar are you with the concept of multi-factor authentication

Select ...

21. How often do you update the software on your computer or mobile device to ensure you have the latest security patches?

Select ...

CYBER SECURITY MITIGATION STRATEGIES DURING THE ATTACK

22 Have you experienced a cyber attack?

Select ...

23 If yes what kind of attack?

Select ...

24 Then, please rate what practices your organization or you see as preventive

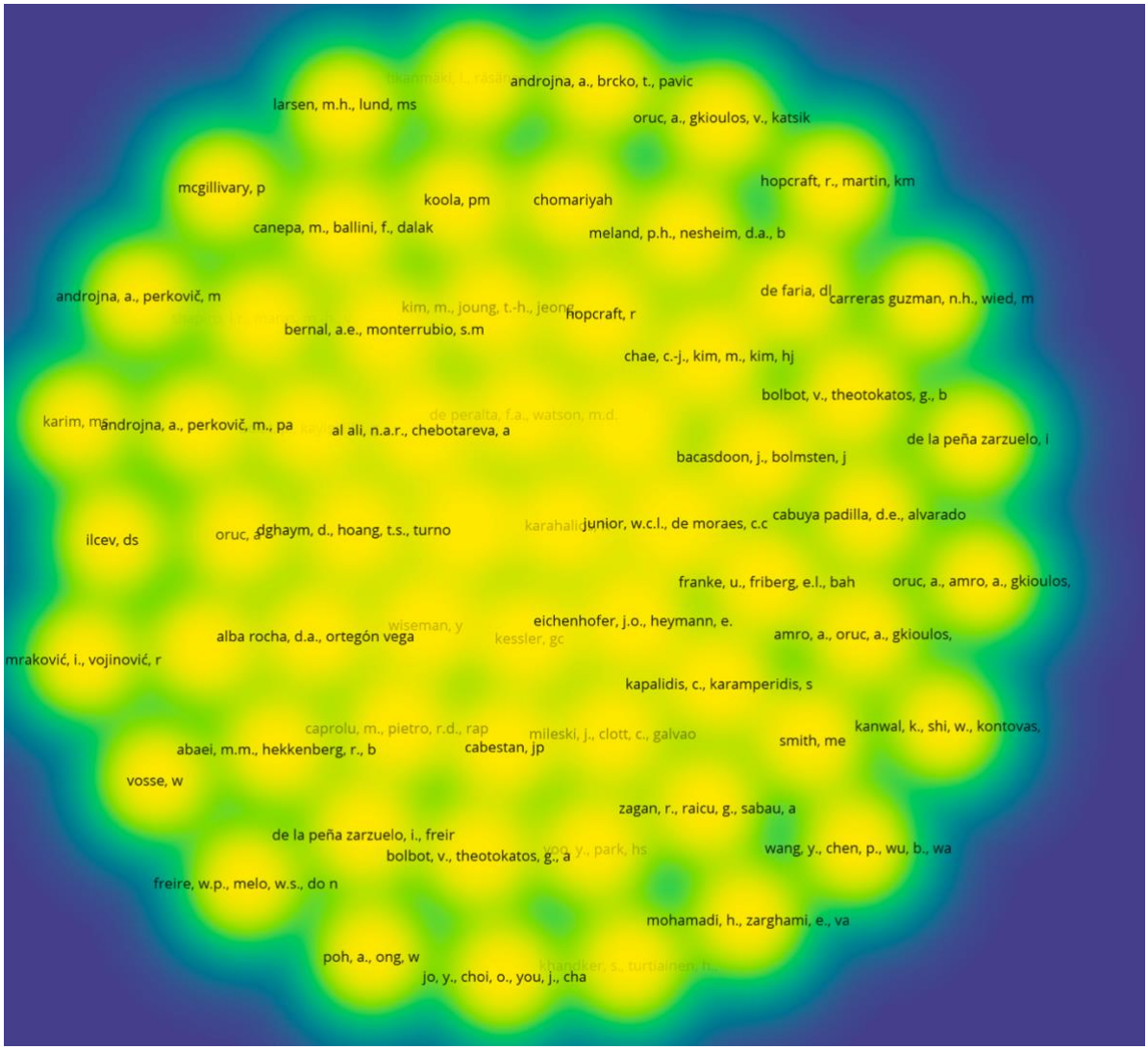
	Very poor	Poor	Medium poor	Fair	Good	Very good
Cyber training and awareness	☐	☐	☐	☐	☐	☐
compliance monitoring in line with legal procedures	☐	☐	☐	☐	☐	☐
Company policy on use of personal devises	☐	☐	☐	☐	☐	☐
Specific company procedures are in accordance to required regulations	☐	☐	☐	☐	☐	☐
Not using personal devises on systems	☐	☐	☐	☐	☐	☐
Aware of the procedures to follow	☐	☐	☐	☐	☐	☐

25 What should your organisation or you do during the attack

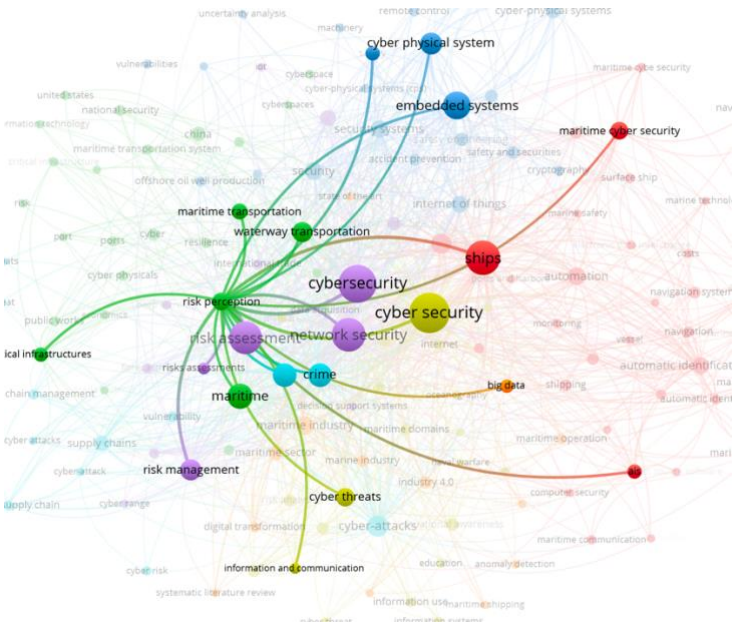
	Very poor	Poor	Medium poor	Fair	good	verygood
Shut down the sysytem	○	○	○	○	○	○
Component isolation	○	○	○	○	○	○
real time monitoring	○	○	○	○	○	○
Task force	○	○	○	○	○	○
Partner interaction	○	○	○	○	○	○

26. In the space provided, write what you or your organisation does after the attack

Appendix 2: a) Literature review



b) Cybersecurity links



c)

25 | fx | To assess cyber-security in maritime annd

No.	Article Title	Year	Journal	Authors	Keywords	Control variables	Purpose of study	Main Findings
1	Cybersecurity: In logistics and supply chain management. An overview of future reseach direction	2021	Transportation Research Part E	Cheung, K.-F., Bell, M. G. H., & Bhattacharjya, J. (2021)	Cybersecurity Defensive measures: Internet of things (IoT). Blockchain Logistics Supply chain	N/A	To review direction of future studies stuidies that explore measures - enhancing cybersecurity in logistics and supply chain management	Scarcity of cybersecurity studeis in logistics Existing studeis rarely use cybersecurity data. Few papers adopt quant. Most studies focus on precautionary measures Very few on real time and after math Studies on IT and digital forensic studies are rare.
2	Estimating economic loses from cyber-attacks on shipping ports: An optimization-based approach.	2022	Transportation Research Part C	Weaver, G. A., Feddersen, B., Marla, L., Wei, D., Rose, A., & Van Moer, M. (2022)	Critical infrastructure; Cybersecurity; Optimization; Ports; Transportation		To understand trade offs shipping stakeholders have to be aware of as they compete in automation. Enables understanding the economic impact of cyberattacks that affect shipping port operationsand thereby enable risk assessment that holistically evaluate interaction among port operations and information technology systems	Results based on cyber attacks on land lord ports and terminal operator assets provided. By Port vergalade, and others illustrate impact of 80-1.2m. USD on average weekly in okt. 2017, and up to 2.4m in may: The runtime performance of DDD algorithm improves performance
	Maritime cybersecurity: are onboard systems ready?		Maritime Policy & Management	Kamlesh Kanwal, Wenming Shi, Christos Kontovas, Zaili Yang & Chia-Hsun Chang (2022)	Cybersecurity, maritime security, human factor,cybercompliance monitoring, structural equation modelling		Evaluating the relationship among the critical dimensions influencing cybersecurity performance in the maritime industry 6 critical dimensions identified through lit: - Regukations, company procedures, trainiag awareness, Hfac, compliance monitoring	(1) provision of useful insights on the important factors that affect cybersecurity performance on ships, which could be further explored in order to identify measures to enhance maritime cybersecurity 2)a new definition of maritime cybersecurity performance, as well as a novel causal relationship framework for modelling maritime cybersecurity factors and performance 3)a number of cybersecurity policy recommendations for the interested parties.
21	STATE OF ART SURVEYS OF OVERVIEWS ON MCDM/MADM METHODS	2022 2014	Technolog ical and economic developm ent OF ECONOMY	Edmundas, Kazmierras, Zenonas	Multicriteria decision making model (MCDM),Multiple objective decision making overview (MODMO)(		Evaluating the relationship among the critical dimensions influencing cybersecurity performance in the maritime industry 6 critical dimensions identified through lit: - Regukations, company procedures, trainiag awareness, Hfac, compliance monitoring	(1) provision of useful insights on the important factors that affect cybersecurity performance on ships, which could be further explored in order to identify measures to enhance maritime cybersecurity 2)a new definition of maritime cybersecurity

DRAFT MATRIX | WAY TO Final Lit matrix | +

Appendix 3 KNOWLEDGE ON CYBER SECURITY INCIDENTS

a)

Descriptive Statistics

	N	Range	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
malware_attacks	22	3	2	5	4.27	.827	−1.1	.491	1.23	.953
phishing	22	3	2	5	4.05	.899	−.96	.491	.722	.953
social_engineering	22	3	2	5	3.77	1.020	−.68	.491	−.46	.953
databreach_consequences	22	2	3	5	4.55	.596	−.93	.491	.025	.953
suspicious_email	22	1	4	5	4.45	.510	.196	.491	−2.2	.953
fake_websites	22	3	2	5	3.73	.827	−.54	.491	.197	.953
unsecured_networks	22	3	2	5	3.68	.945	−.77	.491	−.18	.953
Valid N (listwise)	22									

b)

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
						Significance				95% Confidence Interval of the Difference	
		F	Sig.	t	df	One-Sided p	Two-Sided p	Mean Difference	Std. Error Difference	Lower	Upper
malware_attacks	Equal variances assumed	1.263	.274	.755	20	.230	.459	.274	.362	−.482	1.029
	Equal variances not assumed			.692	12.208	.251	.502	.274	.395	−.585	1.132
phishing	Equal variances assumed	.138	.714	−.760	20	.228	.456	−.299	.394	−1.120	.522
	Equal variances not assumed			−.780	18.791	.223	.445	−.299	.384	−1.103	.504
social_engineering	Equal variances assumed	.469	.501	.397	20	.348	.695	.179	.452	−.763	1.122
	Equal variances not assumed			.388	15.881	.352	.703	.179	.462	−.801	1.160
databreach_consequences	Equal variances assumed	.898	.355	−.065	20	.475	.949	−.017	.265	−.569	.535
	Equal variances not assumed			−.061	13.524	.476	.952	−.017	.282	−.623	.589
suspicious_email	Equal variances assumed	.233	.635	−.766	20	.226	.453	−.171	.223	−.637	.295
	Equal variances not assumed			−.760	16.893	.229	.458	−.171	.225	−.646	.304
fake_websites	Equal variances assumed	.002	.965	−.755	20	.230	.459	−.274	.362	−1.029	.482
	Equal variances not assumed			−.728	15.119	.239	.478	−.274	.376	−1.073	.526
unsecured_networks	Equal variances assumed	.136	.716	.512	20	.307	.614	.214	.417	−.657	1.084
	Equal variances not assumed			.526	18.818	.303	.605	.214	.407	−.638	1.065

c)

Report

gender		malware_attacks	phishing	social_engineering	databreach_consequences
Female	Mean	4.11	4.22	3.67	4.56
	N	9	9	9	9
	Std. Deviation	1.054	.833	1.118	.726
male	Mean	4.38	3.92	3.85	4.54
	N	13	13	13	13
	Std. Deviation	.650	.954	.987	.519
Total	Mean	4.27	4.05	3.77	4.55
	N	22	22	22	22
	Std. Deviation	.827	.899	1.020	.596

d)

Report

work_exp		malware_attacks	phishing	social_engineering	databreach_consequences
0-5yrs	Mean	3.50	3.50	3.00	4.50
	N	2	2	2	2
	Std. Deviation	.707	.707	1.414	.707
11-15	Mean	5.00	4.67	4.67	5.00
	N	3	3	3	3
	Std. Deviation	.000	.577	.577	.000
15++	Mean	4.33	3.67	4.00	4.67
	N	3	3	3	3
	Std. Deviation	.577	1.528	1.000	.577
5	Mean	4.21	4.07	3.64	4.43
	N	14	14	14	14
	Std. Deviation	.893	.829	1.008	.646
Total	Mean	4.27	4.05	3.77	4.55
	N	22	22	22	22
	Std. Deviation	.827	.899	1.020	.596

e)

Report

education		malware_attacks	phishing	social_engineering	databreach_consequences
HS	Mean	4.33	4.17	3.17	4.50
	N	6	6	6	6
	Std. Deviation	.516	1.169	1.169	.548
GR	Mean	4.00	3.83	3.67	4.50
	N	6	6	6	6
	Std. Deviation	1.265	.408	.816	.837
MS	Mean	4.57	4.43	4.29	4.57
	N	7	7	7	7
	Std. Deviation	.787	.787	1.113	.535
PHD	Mean	4.00	3.33	4.00	4.67
	N	3	3	3	3
	Std. Deviation	.000	1.155	.000	.577
Total	Mean	4.27	4.05	3.77	4.55
	N	22	22	22	22
	Std. Deviation	.827	.899	1.020	.596

f)

Report

position		malware_attacks	phishing	social_engineering	databreach_consequences
classification_society_rep	Mean	5.00	5.00	5.00	5.00
	N	1	1	1	1
	Std. Deviation	.	.	.	.
manager_crew	Mean	3.67	3.67	3.67	4.00
	N	3	3	3	3
	Std. Deviation	1.528	.577	.577	1.000
manager_eng_nav	Mean	4.25	4.00	3.50	4.50
	N	4	4	4	4
	Std. Deviation	.957	.000	1.000	.577
others	Mean	4.31	4.08	3.77	4.62
	N	13	13	13	13
	Std. Deviation	.630	1.115	1.166	.506
seafarer_oper	Mean	5.00	4.00	4.00	5.00
	N	1	1	1	1
	Std. Deviation	.	.	.	.
Total	Mean	4.27	4.05	3.77	4.55
	N	22	22	22	22
	Std. Deviation	.827	.899	1.020	.596

Appendix 4. KNOWLEDGE ON CYBER SECURITY RISKS

a)

Frequency Table

knowledge_cyber-sec_risks

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	4.5	4.5	4.5
	2	2	9.1	9.1	13.6
	3	11	50.0	50.0	63.6
	4	7	31.8	31.8	95.5
	5	1	4.5	4.5	100.0
	Total	22	100.0	100.0	

b)

password_intervalupdate

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	4	18.2	18.2	18.2
	3	11	50.0	50.0	68.2
	4	6	27.3	27.3	95.5
	5	1	4.5	4.5	100.0
	Total	22	100.0	100.0	

familiarity_cyberisks

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	4.5	4.5	4.5
	2	2	9.1	9.1	13.6
	3	8	36.4	36.4	50.0
	4	10	45.5	45.5	95.5
	5	1	4.5	4.5	100.0
	Total	22	100.0	100.0	

backup-frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	2	9.1	9.1	9.1
	3	6	27.3	27.3	36.4
	4	11	50.0	50.0	86.4
	5	3	13.6	13.6	100.0
	Total	22	100.0	100.0	

privacy_settings_update_frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	9	40.9	40.9	40.9
	3	7	31.8	31.8	72.7
	4	6	27.3	27.3	100.0
	Total	22	100.0	100.0	

A- 6 Literature Matrix