CYBERSECURITY RISK ASSESSMENT IN THE MARITIME INDUSTRY

CHANGKI PARK

A thesis submitted in partial fulfillment for the degree of
Doctor of Philosophy (PhD)

March 2024

ABSTRACT

Cybersecurity risks are becoming an increasingly significant concern within the maritime industry, particularly in light of the rapid advancement of digitised technologies and the emergence of autonomous shipping. Concurrently, the apprehension surrounding the potential for cybersecurity incidents in maritime settings has also heightened. In fact, the number of reported cases of cyber-attacks in the maritime sector has seen a substantial increase since 2010. Consequently, academic interest in researching maritime cybersecurity has grown, underscoring its importance for a thorough exploration of the subject.

Nevertheless, a scrutiny of existing literature reveals that current cybersecurity research predominantly underscores the necessity for improvement but lacks a specific focus on cyber threats and measures for risk mitigation. Notably, the maritime industry faces a scarcity of comprehensive investigations into cybersecurity risk assessment, and there is also a dearth of scholarly endeavours aimed at establishing a comprehensive framework for evaluating cybersecurity risks relevant to maritime operations.

This thesis aims to create a new framework for assessing cybersecurity risks, contributing to safety improvements in the maritime sector. The objective is to provide a visualised solution that assists stakeholders in understanding and refining their approaches to cybersecurity risk management. Through this innovative framework, the thesis seeks to enhance safety measures and promote effective risk mitigation strategies within the dynamic landscape of the maritime industry.

To attain the research aim, a literature review and bibliometric analysis were conducted to discern maritime cybersecurity guidelines from diverse maritime organisations. This purposed to assess the current state of academic research in the cybersecurity field specific to the maritime sector and address identified research gaps. Subsequently, a systematic literature review was employed to identify various maritime cybersecurity

threats, and cybersecurity risks were assessed using a FMEA-Rule-based Bayesian Network (FMEA-RBN) model.

The next step involved the identification of cybersecurity mitigation measures and criteria through another systematic literature review. These measures were then ranked using the Fuzzy TOPSIS model, enabling the research team to prioritise them effectively. Additionally, the research sought to demonstrate how a bowtie diagram could be integrated into the cybersecurity assessment framework, providing a visual representation of its components. The collective pursuit of these research objectives is anticipated to yield a comprehensive understanding of maritime cybersecurity, contributing to the development of a more efficacious cybersecurity assessment framework tailored for the maritime sector.

Several significances of this research have been proposed. First and foremost, despite numerous studies addressing maritime risk, safety, and security, there remains a notable scarcity of research specifically dedicated to maritime cybersecurity. To bridge this gap, this research systematically identifies various cyber threats in the maritime sector and organises them into distinct groups. This categorisation serves to assist maritime managers in discerning the potential impact of different cyber threats on their cybersecurity management, enabling them to allocate limited budgets more effectively. Secondly, in addition to the identification and assessment of cyber threats, this research puts forth seven risk control measures and six hierarchical criteria for evaluating maritime cybersecurity. This framework aids maritime managers in comprehending the significance of these measures and adapting their cybersecurity strategies to varying circumstances. For example, some companies may prioritise the reliability of measures, while others may place greater emphasis on economic affordability. The research also suggests diverse policies for stakeholders to enhance maritime cybersecurity. Thirdly, this research not only presents a framework for maritime cybersecurity but also conducts risk assessments and evaluates risk control measures using empirical data gathered from industry experts, rather than relying solely on secondary data. This approach provides real-world insights and reflects the current state of maritime

cybersecurity. Lastly, the research introduces a bowtie framework for maritime cybersecurity risk management, demonstrating its application through the assessment of risks related to malware. The visual representation of the bowtie framework assists managers in comprehending maritime cyber threats, potential consequences, and the corresponding risk control measures to mitigate both threats and their consequences.

In conclusion, this thesis significantly contributes to maritime cybersecurity understanding and management, offering practical insights and recommendations for stakeholders to enhance their cybersecurity preparedness and safeguard their operations against cyber threats. The proposed framework and empirical approach ensure their relevance and applicability in the context of current maritime cybersecurity challenges.

ACKNOWLEDGMENTS

This thesis owes its existence to the invaluable help and support of many individuals. I sincerely thank all those who contributed significantly to making this achievement possible.

First and foremost, I extend my heartfelt gratitude to my incredible supervisor team: Dr. Chia-Hsun Chang, Dr. Christos Kontovas, and Professor Zaili Yang. They provided me with the opportunity to pursue my Ph.D. under their guidance and unwavering support. Their belief in my abilities and genuine care contributed to both my academic and personal growth throughout my journey. Their continuous guidance, feedback, and dedication played a crucial role in the success of my research. Their encouragement and invaluable advice helped me overcome challenges and flourish as a researcher and an individual. Their mentorship extended beyond research, offering priceless insights for my career choices. I cannot thank them enough for making my Ph.D. experience truly unforgettable and enriching.

I would also like to convey my deep gratitude to Professor Ki-Chan Nam, Professor Kyu-Seok Kwak, and Professor Hwan-Seong Kim for their inspiring guidance and assistance in facilitating my studies in the UK. Their unwavering support, valuable advice, and encouraging words have been truly priceless.

I extend my thanks to my friends for their support during my studies in Liverpool, especially in tough times. Their mutual encouragement made the journey even more meaningful.

Finally, I want to express my heartfelt appreciation to my parents Joonwon Park (박준원) Malheui Ahn (안말희). Their constant financial and moral support throughout my PhD journey has been invaluable. Moreover, they have served as my lifelong mentors, making significant sacrifices over the years.

Liverpool, October 2023
Changki Park

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

ABS	American Bureau of Shipping
AHP	Analytic Hierarchy Process
AIS	Automatic Identification System
API	American Petroleum Institute
BA	Barrier Analysis
BIMCO	Baltic and International Maritime Council
BN	Bayesian Network
BWM	Best-Worst Method
BYOD	Bring Your Own Device
CL 380	the Institute Cyber Attack Exclusion Clause
CLIA	Cruise Lines International Association
COBIT	Control Objectives for Information and Related Technologies
CPSs	Cyber Physical Systems
CPT	Conditional Probability Table
CRM	Cyber Risk Management
CS	Cyber Security
CSF	Cyber Security Framework
CSM	Cyber Security Management
CV	Crisp Values
DCS	Distributed Control Systems
DCSA	Digital Container Shipping Association
DDoS	Distributed Denial of Service
DMA	Danish Maritime Authority
DNV	Det Norske Verutas
DoB	Degree of Belief
DOC	Document of Compliance

DoS	Denial of Service
EASA	European Union Aviation Safety Agency
ECDIS	Electronic Chart Display and Information System
ENISA	European Union Agency for Cybersecurity
EO	Executive Order
ETA	Event Tree Analysis
EU	European Union
FAA	Federal Aviation Administration
FMEA	Failure Mode and Effects Analysis
FMEA-RBN	Failure Mode and Effects Analysis Rule-based Bayesian Network
FSA	Formal Safety Assessment
FTA	Fault Tree Analysis
GNSS	Global Navigation Satellite System
GPS	Global Positioning Systems
HAZOP	Hazard and Operability Study
HSE	Health and Safety Executive
IACS	International Association of Classification Societies
IAPH	International Association of Ports and Harbours
ICAO	International Civil Aviation Organization
ICS	International Chamber of Shipping
ICSs	Industrial Control Systems
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IMO	International Maritime Organization
INS	Integrated Navigational System
INTERCARGO	International Association of Dry Cargo Shipowners
INTERTANKO	International Association of Independent Tanker Owners
IOGP	International Association of Oil and Gas Producers
IoT	Internet of Things
IRClass	Indian Register of Shipping

IRISL	Islamic Republic of Iran Shipping Line
ISF	Information Security Forum
ISM	International Safety Management
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISPS Code	International Ship and Port Facility Security Code
IT	Information Technology
IUMI	the International Union of Marine Insurance
KR	Korean Register
LOPA	Layer of Protection Analysis
LR	Lloyds Register
MaCRA	Maritime Cyber-Risk Assessment
MCA	Maritime and Coastguard Agency
MCDM	Multiple Criteria Decision Making
MITM	Man in the Middle attack
MLoSC	Maritime Logistics and Supply Chain
MODU	Mobile Offshore Drilling Unit
MOORA	Multi-Objective Optimization by Ratio Analysis
MSA	Maritime Security Assessment
MV-HARM	Maritime Vessel-Hierarchical Attack Representation Model
NIST	National Institute of Standards and Technology
OCIMF	Oil Companies International Marine Forum
OT	Operational Technology
PCI SSC	Payment Card Industry Security Standards Council
PCI DSS	Payment Card Industry Data Security Standard
P&I	Protection and Indemnity Insurance club
PDF	Portable Document Format
PEAR	People Assets Environment Reputation
PSC	Port State Control

PRA	Probabilistic Risk Assessment
QRA	Quantitative Risk Assessment
RBN	Rule-based Bayesian Network
RCMs	Risk Control Measures
RCO	Risk Control Option
RDP	Remote Desk Protocol
RM	Risk Management
RPN	Risk Priority Number
SAMA	Saudi Arabian Monetary Authority
SEPA	Scottish Environment Protection
SMS	Ship safety Management System
SOLAS	Safety of Life at the Sea
SP	Special Publication
SYBASS	Super Yacht Builders Association
TC	Total Citation
TEU	Twenty Foot Equivalent Unit
TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution
UNCTAD	United Nations Conference on Trade and Development
USCG	United States Coast Guard
VIKOR	Vlse Kriterijumska Optimizacija I Kompromisno Resenje
VPN	Virtual Private Network
WASPAS	Weighted Aggregated Sum Product Assessment
WSC	World Shipping Council

1

INTRODUCTION

1.1 Background: The Maritime Industry and Safety Regulations

Maritime history dates back thousands of years, as there is evidence of trade using ships between ancient civilisations. There is no better way to summarise the importance of maritime transportation than using the well-worn expression, "*With over 80 per cent of global trade by volume and more than 70 per cent of its value being carried on board ships and handled by seaports worldwide, the importance of maritime transport for trade and development cannot be overemphasised*" (UNCTAD, 2017). This phrase also captures well the characteristics of maritime transportation, i.e., mainly used for less valuable cargo (more expensive cargo is carried mainly using aeroplanes) and oversized shipments. Ships are, therefore, the main enablers of international transportation.

According to the latest Review of Maritime Transport (UNCTAD, 2022), which is published by the United Nations Conference on Trade and Development (UNCTAD), international seaborne trade in 2021 was responsible for carrying 11 billion tons; container port traffic alone was estimated at 857 million TEUs.

It has been early recognised that shipping is a truly international industry. The need to operate effectively and to maintain a level playing field has led to the belief that this can only be done *"if the regulations and standards are themselves agreed, adopted and implemented on an international basis".* The main forum for this is the International Maritime Organization (IMO)- which is a United Nations agency. The IMO was

established through a Convention that was adopted in Geneva in 1948 and entered into force in 1958 (the original name was the Inter-Governmental Maritime Consultative Organization or IMCO, but the name was changed to IMO in 1982).

While there was evidence that the IMO Conventions helped reduce the number of accidents and improve overall maritime safety, it has been argued see, for example, by Kontovas and Psaraftis (2009), that much of maritime safety policy has been developed in the aftermath of serious accidents (such as Exxon Valdez, Estonia, Erika, and Prestige). They questioned this practice, stating, *"Why should the maritime industry and, in general, society have to wait for an accident to occur to modify existing rules or propose new ones? ".*

The international shipping industry has transitioned from a reactive to a proactive approach to safety, known as 'Formal Safety Assessment' (FSA). FSA was initially developed partly as a response to the Piper Alpha disaster in 1988 when an offshore platform exploded in the North Sea, and 167 people died. In 1993, following a proposal by the UK's Maritime and Coastguard Agency (MCA), the IMO started working on a set of guidelines, and in 1997 they approved the 'Interim Guidelines for the application of Formal Safety Assessment to the IMO rulemaking process'. The guidelines have been amended a number of times and have now been superseded by MSC-MEPC.2/Circ.12/Rev.2 (IMO, 2018).

FSA is now IMO's primary risk assessment tool. Its purpose is *"a structured and systematic methodology, aimed at enhancing maritime safety, including protection of life, health, the marine environment and property, by using risk analysis and cost-benefit assessment*" (IMO, 2018); see Section 2.3.2 for more. As will be seen later on, FSA follows a typical risk assessment methodology and is in line with the International Organization for Standardization (ISO) ISO 31000 Risk Management family of standards.

1.2 Background: Maritime Cybersecurity

Based on the above, neither the IMO Convention nor the FSA risk assessment process specifically mention security-related issues. However, the IMO started working much on maritime security, especially in response to perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States and 2002. According to its International Ship and Port Facility Security Code (ISPS Code), which is implemented through chapter XI-2 of the SOLAS Convention, measures have been adopted to *"enhance ship and port facility security."* For more information, see Section 2.5.

Security issues are also at the centre stage of IMO's work and a major concern of the shipping industry. It should note here that there is much work on preventing piracy and armed robbery against ships, counterterrorism, stowaways, drug smuggling and other concerns; however, these are out of the scope of this work.

In recent years, the maritime industry has grown increasingly concerned about cybersecurity, a modern security aspect. This is primarily due to factors like the expanding use of Information Technology (IT) systems, automation, and digitisation. Onboard vessels, software and hardware systems now play a crucial role in controlling various processes, including navigation, engine and power management, and damage control systems monitoring. Furthermore, digital connectivity, particularly online communication access, is of paramount importance to seafarers as it is closely linked to their well-being, crew cohesion, and avoidance of social isolation.

Thus, cybersecurity plays an extremely important role in the maritime industry to maintain well-functioning business operations and to mitigate the negative impact of malicious cyberattacks. Failure to address cyberattacks in the maritime sector could result in severe consequences, including human fatalities, asset and reputation loss, economic damages, and environmental repercussions.

Many maritime cyberattacks have been reported since the early 2010s; see Table 1-1 and 1-2 for a detailed list of maritime cybersecurity accidents. Recent representative incidents include (a) the 2020 ransomware attack that hit the servers of container shipping giant CMA CGM, leading to the company's main website and applications being temporarily inaccessible (Shen and Baker, 2021), (b) the sophisticated cyberattack which affected the International Maritime Organisation's (IMO) IT systems including the public web site and its internal intranet systems (O'Dwyer, 2020).), and (c) the damage of equipment and information of containers by a cyberattack in a South Africa container operation company in July 2021 (Shead, 2021).

It can, therefore, be said that there has been a number of significant incidents, some of which have enormous consequences, also in financial terms. Perhaps the most well-known case is the 2017 ransomware attack on Maersk, which led to a financial loss estimated at $200-300 million due to a three-week network system shutdown (The Maritime Executive,2021a).

To respond to the increasing concerns on maritime cybersecurity, the IMO and the Baltic and International Maritime Council (BIMCO) - one of the world's major shipping associations have led the relevant discussions at an international level, which resulted in the publication of the first-ever maritime cybersecurity guidelines (BIMCO, 2016).

Table 1-1: Maritime cyberattack incidents

Year	Organisation	Description
2011	IRISL	The system of this Iranian shipping line was hacked, and lost confidential data such as delivery fee, number of cargos, date of departure and port of departure and destination (Torbari and Saul, 2012).
2011-2012	Port of Antwerp	The IT system of the Port of Antwerp was hacked by drug traffickers. They obtained the location of containers with heroin and cocaine. It is found that some malicious software was emailed to port staff, allowing the drug traffickers to access data remotely (BBC News, 2013).
2012-2014	Danish Maritime Authority (DMA)	The cyberattack on DMA started in 2012 and was discovered in 2014. It was found that a PDF document was infected with a virus, which propagated from DMA to other government organisations (Linton Art, 2016).
2013	Mobile Offshore Drilling Unit	A group of hackers remotely controlled the stabilisation system of a floating oil rig in the Gulf of Mexico and attempted to tilt the platform to one side using malware software. This caused the system to shut down for 19 days (MODU, 2013).
2016	South Korean vessels	The government reported that North Korean organisations jammed 280 vessels' GPS signals; consequently, some of the vessels' GPS signals lost their location, and others received wrong information (Polychronis, 2020).
2017	Maersk	Maersk's network system was shut down by ransomware (NotPetya). Maersk took almost three weeks to recover the system and thus caused a $200-300 million financial loss (The Maritime Executive,2021a).
2017	Clarskon Plc	An unauthorised third party gained access to the company's computer systems in the UK, copied data, and demanded a ransom for its return. Fortunately, all the illegally stolen data was successfully recovered through investigation and legal measures. (ASC Staff, 2017).
2018	COSCO terminal at Port of Long Beach	COSCO terminal at the port of Long Beach was attacked by malware. It took five days to recover the system, yet COSCO did not suffer severe financial loss by separating its network into different servers (COSCO World Maritime News, 2018).
2018	Port of Barcelona	The servers were cyberattacked by ransomware, which influenced their security infrastructure. There was negligible damage due to the port administration having developed a sound cybersecurity plan (ISN,2018).
2018	San Diego Port	Just five days after the Port of Barcelona accident, the San Diego port also was cyberattacked by ransomware. There was an impact on the internal IT system and land operations, such as vessel loading or unloading (BBC News, 2018).
2018	Australian shipbuilder	Australian defence shipbuilder Austal announced it had been the victim of malware, resulting in the theft of unclassified ship designs, which were later sold online (Reynolds,2018).
2018	U.S Navy	US Navy officials reported that Chinese hackers had stolen information about missile projects from Navy contractors (Volz, 2019).
2019	U.S merchant ship	The US Coast Guard has reported that malware attacks had a significant effect of degrading the function of the onboard control system network (Rundle, 2019).
2019	James Fisher and Sons	UK-based Marine service provider company informed that its computer systems had suffered an unauthorised intrusion. They disconnected from communication and financial systems while they recovered (Goud, 2019).
2019-2020	Carnival Corporation and plc	Carnival Corporation and plc, a cruise operator, has suffered two ransomware attacks in two years, resulting in the theft of personal information and credit card details of customers and employees. The details of the virus and mode of attack have not been disclosed, but the company has warned of potential compensation claims from affected parties (The Maritime Executive, 2020a).

Table 1-2: Maritime cyberattack incidents (continued)

Year	Organisation	Description
2020	CMA-CGM	The network system was cyberattacked by ransomware. To deal with such attacks, CMA-CGM blocked their e-commerce website to protect customers (Shen and Baker, 2021).
2020	IMO	The website and intranet were attacked by a sophisticated cyberattack suspected of being ransomware. This caused limited access until systems were recovered (O'Dwyer, 2020).
2020	MSC	MSC, a shipping company based in Geneva, Switzerland, suffered an attack by a ransomware virus, resulting in the closure of its headquarters for a period of five days (Goud, 2020).
2020	Matson shipping company	Matson, a transportation and shipping company based in the United States, has reported a system outage caused by a cyberattack. While the attack has not disrupted cargo operations, certain transactions have been delayed as the affected functions need to be manually processed (Omnitrans, 2020).
2020	Port of Kennewick	The IT systems of the Port of Kennewick were rendered unusable by a ransomware attack, following which the hackers demanded a ransom of 200,000 USD. However, the ransom was not paid, and the systems remained unavailable for several days until they could be restored from offline backups (TCAJOB Staff, 2020).
2020	Hurtigruten cruise	Hurtigruten, a Norwegian cruise operator, experienced a significant ransomware attack that had a severe impact on its IT infrastructure, resulting in the unavailability of multiple critical systems for several days. The incident also led to the exposure of passenger data, including passport information, which may have been compromised (The Maritime Executive, 2020b).
2020	AIDA cruise	AIDA, a German cruise operator based in Rostock, suffered an attack by the DoppelPaymer ransomware, which led to significant IT issues, ultimately forcing the company to cancel a number of scheduled cruises (The Maritime Executive, 2020c).
2021	Transnet	The online system of this South African container terminal operator was cyberattacked, which caused data and financial loss (Shabalala and Heiberg, 2021).
2021	Greek shipping companies	Several Greek shipping companies suffered a ransomware attack in 2021 that spread through the systems of an IT consulting firm (The Maritime Executive, 2021 b).
2022	European oil port terminal	Oil loading facilities in Germany and spread to key terminals in the Amsterdam-Rotterdam-Antwerp network. There was a cyberattack at various terminals, and quite some terminals were disrupted due to their software being suffered and the operational system being down (BBC News, 2022).
2022	Port of Lisbon	Port of Lisbon's website and international computer system has been shut down due to a cyberattack. Hacker groups announced that vital port-related data are stolen, such as financial reports, audits, budgets, contracts, cargo information etc. (The Maritime Executive, 2022).
2023	DNV	DNV has reported that around 70 companies and 1,000 vessels could have been affected by ransomware incident and shut down the IT servers connected to their Ship Manager system (The Record, 2023).
2023	DP world	The Australia's largest port operator, DP world Australia, has been targeted cyber-attack in November. They disconnected their intranet, and closed Sydney, Melbourne, Brisbane and Fremantle port operations after detecting cyberattack. (The Guardian, 2023)

In 2017, the IMO adopted its first 'Maritime Cyber Risk Management' guidelines (IMO, 2017a), which were largely based on industry-led work published by BIMCO (BIMCO, 2016). These guidelines, known as “Maritime Cyber Risk Management”, MSC-FAL.1/Circ.3, marked the IMO's initial step in addressing cybersecurity concerns, and they were introduced in July 2017 (IMO, 2017a). According to the Guidelines, maritime cyber risk refers to *"a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised"* (IMO,2017a). Furthermore, the IMO (2017b) adopted a resolution that "*encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the International Safety Management (ISM) Code) no later than the first annual verification of the company's Document of Compliance (DOC) after January 1, 2021*". Note that ISM code provides an international standard for safe vessel management and operations at sea. Since 2021, shipowners and operators must comply with and address cyber risks in their existing safety management systems.

The Guidelines highlight the fact that cybertechnologies are now *"essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment".* The IMO proposes the use of risk management – which, as see in the case of Formal Safety Assessment – is fundamental to safe and secure shipping operations. There have been indeed a number of cyber security incidents (see Table 1-1 and 1-2) demonstrating the need to address the relevant threats. As per the guidelines – and in line with well-established risk management frameworks such as ones presented in the ISO standards – IMO proposes a risk management approach focusing on the identification of threats, the implementation of risk control processes and measures, the development and implementation of activities and plans to detect cyber-events in a timely manner and respond to them in order to ensure resilience and fast recovery.

Around the same time, leading classification societies and maritime authorities developed guidelines related to cyber risk. For example, DNV (2016) presented guidance (i.e., recommended practices) for ships and mobile offshore operations to improve their cybersecurity resilience management. Amongst others, it proposed an approach based on a bowtie method to analyse the robustness of barriers against threats. The American Bureau of Shipping (ABS, 2016) released its "Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations" document, which provides guidelines for marine and offshore cybersecurity practices. In addition to the documents published by classification societies, a number of maritime administrators have revealed issues on how shipowners could comply with the regulations (both national and international).

A review of the relevant literature is presented in literature review part. This includes scholarly articles; the relevant literature is relatively scarce, but also several relevant ISO standards, IMO-related work, industry standards and guidelines, including the guidelines drafted by Classification Societies. The literature identified a gap in providing concrete and prescriptive methods to address the relevant risks. This is also the case for the BIMCO-led Guidelines *"explain why and how cyber risks should be managed in a shipping context,"* but the 'how' is not that specific in that no specific tools are described.

At the same time, for example, Class societies present a number of different approaches (see Section 2.6). Most guidelines provide high-level recommendations for maritime cyber risk management, perhaps recognising that, as highlighted in MSC-FAL.1/Circ.3, *"no two organisations in the shipping industry are the same, these Guidelines are expressed in broad terms in order to have a widespread application".*

However, recognising the need for more solid and scientific approaches, and the limited scientific literature related to maritime cybersecurity, the author undertook the task of performing research related to assessing the maritime related cyber threats. To that extent, the following aims and objectives have been formulated.

1.3 Research Aim and Objectives

The maritime industry faces significant challenges in terms of cybersecurity, making it imperative to enhance awareness and adopt appropriate measures to mitigate cyber risks. This research aims to develop a comprehensive framework for managing cybersecurity risks within the maritime sector, which can serve as a foundational reference for subsequent research endeavours. The proposed framework will offer a systematic methodology for identifying, evaluating, and addressing cyber risks specific to the maritime industry. Furthermore, it will facilitate coordinated and comprehensive research efforts, thereby ensuring a holistic approach to maritime cybersecurity.

To achieve the research aim, five research objectives are proposed as follows:

Research Objective 1: To conduct a literature review and bibliometric analysis to identify maritime cybersecurity guidelines from various maritime organisations. Additionally, the study assesses the current state of academic research in the cybersecurity field within the maritime sector. The purpose of this comprehensive review is to illuminate the cybersecurity challenges and issues facing the maritime industry.

Research Objective 2: To evaluate cybersecurity risk using a FMEA Rule-based Bayesian Network (FMEA-RBN) model. Several maritime cybersecurity threats are identified through a systematic literature review, and their significance is assessed through interviews with experts and surveys, evaluating their likelihood and consequences using the developed BN.

Research Objective 3: To identify cybersecurity mitigation measures and criteria through a systematic literature review.

Research Objective 4: To rank the mitigation measures using the fuzzy TOPSIS model. This model will enable the research team to prioritise the mitigation measures.

Research Objective 5: To illustrate how a bowtie diagram could be used within the cybersecurity assessment framework. This diagram will offer a visual representation of the framework and its components.

It is believed that these research objectives will provide a comprehensive understanding of maritime cybersecurity and aid in the development of a more effective cybersecurity assessment framework for the maritime sector.

1.4 Research Gap and Significance of This Research

In line with the content outlined in Section 1.2, there has been a noticeable increase in cybersecurity incidents within the maritime domain. This underscores the growing urgency to strengthen cybersecurity protocols and bolster corresponding protective strategies. Consequently, the field of inquiry regarding cybersecurity issues within the maritime sector is still in its early stages. Using a traditional safety-based approach, such as FSA, to address maritime cybersecurity risks is limited and complex. There is a need for a new way of thinking to access maritime cybersecurity.

Current research in cybersecurity primarily emphasises the need for improvement but lacks a specific focus on cyber threats and risk mitigation measures. The maritime industry, in particular, suffers from a dearth of comprehensive investigations into cybersecurity risk assessment. There is also a shortage of scholarly efforts to establish a comprehensive framework for evaluating cybersecurity risks relevant to maritime operations.

In this context, there is a notable absence of well-established methods for quantifying and assessing maritime cybersecurity risks. Additionally, tools or methods to connect high-risk cybersecurity threats with appropriate countermeasures are lacking, as are visualisation solutions, especially within the maritime sector. Consequently, research in cybersecurity for maritime operations is still in its infancy. Most existing studies concentrate on enhancing general cybersecurity measures, with limited attention given to individual cyber threats and strategies for reducing associated risks. This gap extends to the scarcity of scholarly endeavours aimed at devising a comprehensive framework for evaluating cybersecurity risks in maritime operations.

In this research, a comprehensive examination of cyber threats specific to the maritime sector has been conducted, along with the corresponding risk control measures. To enhance effective risk management, a bowtie framework for maritime cybersecurity risk management has been proposed. This framework offers a visual representation of maritime cyber threats, their potential consequences, and the essential risk control measures required to mitigate these threats and their associated consequences. Consequently, the bowtie framework can serve as an innovative model for future research initiatives seeking to develop a more comprehensive framework for maritime cybersecurity. By utilising the visual representation provided by the bowtie framework, managers and stakeholders can easily comprehend the nature of maritime cyber threats, evaluate potential consequences, and implement the necessary risk control measures to effectively mitigate these threats. Given the above, further exploration of existing literature in this field is imperative. It is anticipated that cybersecurity will attract increasing research attention, particularly as the body of literature on autonomous shipping continues to expand. As the level of autonomy increases, so too will the dependence of ships on IT and OT systems, thereby heightening overall cybersecurity risks.

1.5 Structure of This Thesis

This research consists of six chapters to achieve research objectives; see Figure 1-1.

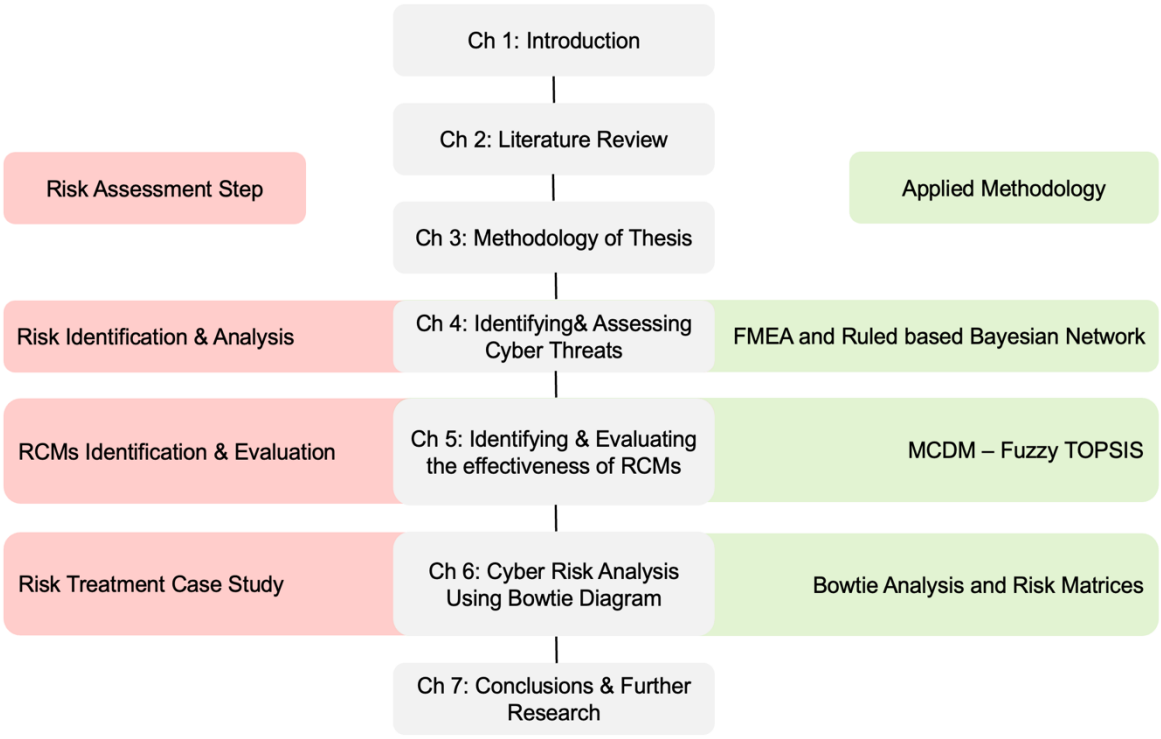


Figure 1-1: Structure of the PhD thesis illustrating main methods

Chapter 1 introduces the research topic, outlines the research aims and objectives, discusses the significance of the research, and provides an overview of the thesis structure.

Chapter 2 presents a definition of risk and risk-related vocabulary (Section 2.1), relevant safety-based risk management frameworks (Section 2.3), and cybersecurity-related ones (Section 2.4), as well as much discussion on relevant industry and regulatory approaches. This is followed by an extensive bibliometric analysis and literature review of the academic literature (Section 2.9)

Chapter 3 outlines the methodology employed in this thesis. It elucidates the research design, details the data collection process, explains the steps of analysis and validation, and discusses the reliability of the model. Moreover, this chapter provides justification for the use of the methodology in each technical chapter.

Chapter 4 aims on assessing cybersecurity risks in the maritime sector. It begins with a thorough literature review that identifies various maritime cyber threats. The chapter then introduces a hybrid method that combines Failure Mode and Effects Analysis (FMEA) with a Rule-based Bayesian Network (RBN) to evaluate the risk levels of these identified threats and gain a deeper understanding of the threats contributing the most to overall maritime cybersecurity risk.

Chapter 5 focuses on the measures to reduce the relevant risks. A framework that can be used to assess cybersecurity mitigation measures is presented. Fuzzy TOPSIS (Technique for Order Performance by Similarity to Ideal Solution), one of the most well-known classical multicriteria decision-making analysis techniques (MCDA) methods, is utilised to rank the most viable measures based on the opinion provided by experts.

Chapter 6 describes the bowtie analysis as a tool to identify robust barriers that can effectively mitigate and reduce the impact of cyberattacks in advance in the maritime sector. The conceptualisation of a bowtie-based framework for maritime cybersecurity risk assessment is presented (Section 5.5.), followed by an illustration of how this could be applied.

Chapter 7 summarises the overall results and main findings of the study and points out the further research direction.

2

LITERATURE REVIEW

2.1 Definition of Risk and Risk-related Vocabulary

Undoubtedly, the most important notion in assessing and managing risk- both in the traditional safety domain and related to cyber security- is that of 'risk'. However, there needs to be a more straightforward definition of the relevant vocabulary; this is also the case for the traditional safety domain; see, for example, Aven (2010) on a discussion of the different definitions and aspects of risk.

This section aims to present the various terms used in the cybersecurity domain, drawing from definitions used in traditional safety and security. This is an essential step as this helps us understand whether the traditional safety risk assessment techniques could be extended to address security-related risks, especially cybersecurity-related ones.

Kaplan and Garrick (1981), in a paper that has strongly influenced the conceptualisation of engineering risk, define risk as a 'set of triplets', a set of scenarios (Si), each of which has a probability (Pi) and a consequence (Xi). Furthermore, their approach is to use the frequency with which an event might occur, which is essentially the notion of uncertainty about the frequency, which is the 'probability of frequency'. Therefore, a risk analysis (which is a part of risk assessment) tries to answer the following questions (Kaplan and Garrick, 1981): (i) What can happen, (ii) How likely is it to happen? and (iii) Given that it occurs, what are the consequences?

According to the ISO terminology (ISO 31073:2022 'Risk management — Vocabulary'), the pivotal definition of risk is the *“effect of uncertainty on objectives”*, the objectives being defined as *“the results to be achieved”*. This definition recognises the surrounding uncertainty - the "state, even partial, of deficiency of information related to understanding or knowledge". It further notes, "*Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood*”.

To fully understand the above definition, it should be looked at its various components per the ISO 31073:2022 definitions; a similar approach has been used in ISO Guide 73:2009. A risk source is defined as an *"element which alone or in combination has the potential to give rise to risk".* An event can be a risk source; it is something that is expected, which might not happen, or something not expected, which might happen. At the same time, the ISO definition note that an event can *"have one or more occurrences, and can have several causes and several consequences".* The consequence is defined as the *"outcome of an event affecting objectives"* and it is noted that they can be qualitative or quantitative and can have positive or negative, direct or indirect, effects on objectives.

The trickiest part is related to the definition of likelihood. The standard states that in risk management terminology, the word 'likelihood' is used to refer *to "the chance of something happening”*, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically, such as a probability (i.e., *“measure of the chance of occurrence expressed as a number from 0 to 1, where 0 is impossibility and 1 is absolute certainty”*) or a frequency (i.e., *“number of events or outcomes per defined unit of time”*).

Note that the above definition of risk needs to consider the various 'threats' and 'vulnerabilities' - terms that are central in the definition of risk in the security context; see below. At the same time, the ISO standard differentiates between hazards and threats; a hazard is defined as a *"source of potential har*m" and a threat as a *"potential source of danger, harm, or other undesirable outcome".*

One might analyse, assess and manage security-related risks using traditional safety approaches. in the maritime domain, this could be, for instance, the Formal Safety Assessment (FSA). An example of how this can be achieved has been illustrated by Yang et al. (2014), who propose a Maritime Security Assessment (MSA) framework based on FSA. The initial step in this framework is the 'identification of threats and vulnerabilities'.

It is worth noting that addressing security-related risks using safety-based risk assessment and management techniques is not straightforward. Unified frameworks have also been proposed; for example, Aven (2007) presents risk and vulnerability management frameworks dealing with accidental (safety) events and security problems. In their work, a clear distinction between risk and vulnerability (which is central in addressing security risks) has been made; risk is defined as *"the combination of sources (including associated uncertainties) and vulnerabilities".*

Based on the above, it is evident that the notion of vulnerability is central in dealing with security risks and, to that extent, cybersecurity risks; see the frameworks presented in Section 2.4. It is apparent that tools and frameworks that address cybersecurity risks are heavily influenced by and follow, in fact, the same rationale as those that address security-related risks and are more specifically related to Information Technology (IT) security. As will be pointed out later, much of the maritime-related research draws from work which adapts IT-related research to the maritime domain; many of the approaches might not be fit for purpose and are also much outside the traditional maritime safety way of thinking.

In addressing IT security risks, the International Organization for Standardization (ISO) has developed with the International Electrotechnical Commission (IEC), an international standards organisation that prepares and publishes international standards for all electrical, electronic, and related technologies, the ISO/IEC 27000 series of standards. IMO itself (as per MSC-FAL.1/Circ.3, which has been discussed in the Introduction) refers the interested parties seeking detailed guidance on cyber risk management, among others, to the ISO/IEC 27001 standard; see Section 2.4.3. ISO/IEC

27000:2018, which provides the definitions for the Information Security Management system (ISMS) family of standards, defines risk in a similar way to that of ISO 31073:2022 (and also ISO Guide 73:2009 which ISO/IEC 27000:2018 actually references) but, in addition, it notes that *"Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization"*.

The widely used in the maritime domain industry-led 'Guidelines on Cyber Security Onboard Ships' define risk as "the product of Likelihood (i.e., the product of the threat and the vulnerability) and Impact"; see Figure 2-1.

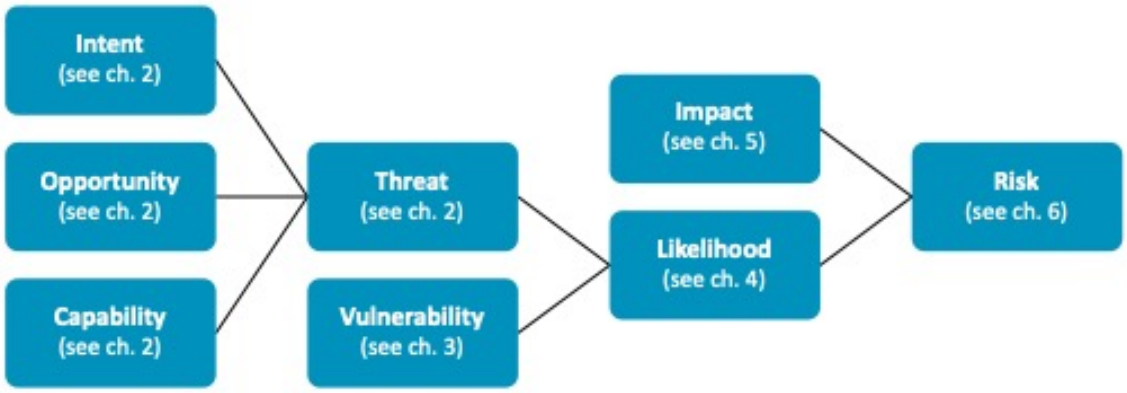


Figure 2-1: The relationship between different factors influencing the risk. - Source: BIMCO (2020)

The lines represent multiplication, and the chapter numbers refer to the BIMCO Guidelines' corresponding chapter.

Table 2-1 below presents the various risk-related definitions per the relevant maritime-related cyber security (CS) risk management (CRM) guidelines/frameworks. Note that most definitions, except for the ISO/IEC standards, are not provided directly in the relevant text.

Table 2-1: Cybersecurity risk related definitions - Source: Author based on stated guidelines/standards

IMO Guidelines MSC-FAL.1/Circ.3	
CRM	*"the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders"*
Risk	*"may result from vulnerabilities arising from inadequate operation, integration, maintenance and design of cyber-related systems, and from intentional and unintentional cyberthreats"*
Threat	*"Threats are presented by malicious actions (e.g., hacking or introduction of malware) or the unintended consequences of benign actions (e.g., software maintenance or user permissions)"*
Vulnerability	Threats expose or exploit vulnerabilities, *which "can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyber discipline"*
BIMCO Guidelines v4	
CRM	*Same as in the IMO Guidelines*
Risk	Risk is the product of Likelihood (i.e., the product of the threat and the vulnerability) and Impact
Threat	*"Threat is the product of the threat actor's capability, opportunity and intent to cause harm"*
Vulnerability	*"weakness that could be leveraged by potential threats "*
US NIST Cybersecurity Framework v. 1.1	
CRM	**RM:** The process of identifying, assessing, and responding to risk. **CS:** The process of protecting information by preventing, detecting, and responding to attacks. Cyber SCRM is *"the set of activities necessary to manage cybersecurity risk associated with external parties."*
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Threat (NIST SP 800-53 Rev. 4) or Cyberthreat (NIST SP 800-128)	*n/a - reference to ISO/IEC 27001:2013 and NIST SP 800-53 Rev. 4 "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service."*
Vulnerability	*n/a - reference to ISO/IEC 27001:2013 and NIST SP 800-53 Rev. 4 "Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."*
Cybersecurity event	*"A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)."*

Table 2-2: Cybersecurity risk related definitions continued - Source: Author based on stated guidelines/standards

BS EN ISO/IEC 27000:2020 Information security management	
RM	*"coordinated activities to direct and control an organization (i.e. person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives) with regard to risk"* [SOURCE: ISO Guide 73:2009]
Risk	*"effect of uncertainty on objectives"* *Note 1: An effect is a deviation from the expected — positive or negative.* *Note 2: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.* *Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.* *Note 5 to entry: Information security risks can be expressed as effect of uncertainty on information security objectives.* *Note 6 to entry: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization."*
Threat	*"potential cause of an unwanted incident, which can result in harm to a system or organization"*
Vulnerability	weakness of an asset or control (i.e., measure that is modifying risk) that can be exploited by one or more threats
Event	*"occurrence or change of a particular set of circumstances"* Notes: An event can be one or more occurrences, and can have several causes. An event can consist of something not happening and sometimes be referred to as an "incident" or "accident"
RM	*"coordinated activities to direct and control an organization (i.e. person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives) with regard to risk"* [Source: ISO Guide 73:2009]

2.2 Definition of Cybersecurity and Cybersecurity Management

Cyber security management (CSM) is defined both in IMO doc. MSC-FAL.1/Circ.3 (IMO, 2017a) and the BIMCO Guidelines vol.4 (BIMCO, 2020) as *"the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders".*

Other definitions per the industry standards and guidelines are shown in Table 2-1 and 2-2.

Various definitions can also be found in the literature (see below).

According to Von Solms and Van Niekerk (2013), cybersecurity protects cyberspace and individuals and organisations that function within cyberspace and their assets in that space.

National Institute of Standards and Technology (NIST, 2015) defines cybersecurity as "*the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems*".

Mission Secure (2021) define maritime cybersecurity as *"the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies used to protect maritime organisations, their vessels, and their cyber environment"* (Mission secure, 2021).

Park et al. (2023) defines maritime cybersecurity using the FMEA-RBN approach. They addressed the maritime cybersecurity definition with five levels for three different parameters following: Likelihood, Consequence, and Probability of the being undetected for maritime cybersecurity. It is illustrated in detail in section 4.3.1.

In addition, in Section 4.3.1, our definition of cyber risk is presented by employing the FMEA risk priority number, which considers the likelihood of a cyber threat, its detectability, and consequences.

A number of relevant risk management frameworks related to both safety and cybersecurity that have been widely utilised in the maritime domain and other industries will now be presented in next section.

2.3 Safety-Related Risk Management Frameworks

The origins of risk assessment, especially of the quantitative approaches used in the engineering and maritime domain, dates back to the early 1970s. One of the first examples is the comprehensive study, also referred to as the 'Reactor Safety Study' (WASH-1400), which was published in 1975 for the US Atomic Energy Commission and described the risks of a nuclear plant. Since then, similar methodologies have been produced; see, for example, the probabilistic risk assessment (PRA) of space systems and quantitative risk assessment (QRA) in the offshore oil and gas industry and assessments of human and environmental risk from chemicals (Kontovas, 2011). Most risk assessment/management frameworks share a common ground; they are in line with ISO standard 31000, which present guidelines for risk management and apply techniques as the ones presented in IEC 31010:2019. These are very generic frameworks and approaches that have broad applications and have been used in various industries mainly to assess safety and environmental protection risks.

2.3.1 ISO 31000 and IEC 31010

In 2009, a new ISO standard (ISO 31000:2009) came together with a new associated vocabulary/terminology (ISO Guide 73:2009) and IEC 31010:2009, a supporting standard for ISO 31000 that guides the selection and application of systematic techniques for risk assessment. The industry has widely used these standards and is now superseded by newer versions, ISO 31000:2018 and IEC 31010:2019.

Per ISO 31000:2018, the risk management process involves "the systematic application of policies, procedures and practices to communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk", illustrated in Figure 2-2.

Risk assessment is the overall process of risk identification, analysis, and evaluation. Risk identification aims to *"find, recognize and describe risks that might help or prevent an organization achieving its objectives".*

Risk analysis: The next step is to analyse the risk- that is, to *"comprehend the nature of risk and its characteristics including, where appropriate, the level of risk".* In doing so, a quantitative approach could also be used; quantifying the risks is not easy as it involves determining the consequences and their likelihood.

Risk evaluation: Evaluating the levels of risk is the process of determining whether the risk and/or its magnitude is acceptable or tolerable, which again is not straightforward as it is required to define the level of risk which is acceptable.

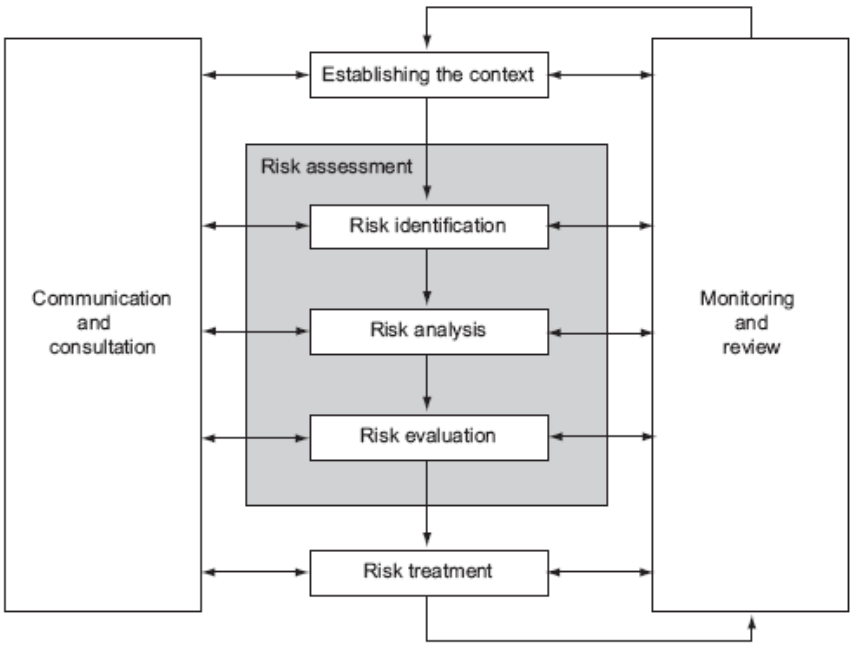


Figure 2-2: Risk Management Process - Source: ISO (2009)

Note: Figure comes from ISO 31000:2009; this has now been superseded by ISO 31000:2018

Risk assessment can be used as a standalone tool or part of a more exhaustive risk management process, where decision-makers can look at the level of risks and measures that can, for example, reduce them, if required.

This is referred to as risk treatment and involves looking at various actions/optics that can perform one or more of the following (ISO 31000:2018):

- *"avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;*
- *taking or increasing the risk in order to pursue an opportunity;*
- *removing the risk source;*
- *changing the likelihood;*
- *changing the consequences;*
- *sharing the risk (e.g., through contracts, buying insurance);*
- *retaining the risk by informed decision."*

According to the ISO standard, *"justification for risk treatment is broader than solely economic considerations",* meaning that decision-makers should not only make decisions based on, for example, whether the costs of implementing a risk control option are less than the benefits gained (cost-benefit analysis) but *"should take into account all of the organization's obligations, voluntary commitments and stakeholder views"*.

Other important considerations of the process include the ongoing monitoring and periodic review of the risk management process (after all many risks are very dynamic), as well as the communication within the organisation and the relevant stakeholders.

2.3.2 IMO Formal Safety Assessment

Formal Safety Assessment (FSA) was introduced in 2002 by the International Maritime Organization (IMO) as a rational and systematic process for assessing risk. According to the latest version of the Guidelines (see IMO doc. MSC-MEPC.2/Circ.12/Rev.2), FSA is *"a structured and systematic methodology, aimed at enhancing maritime safety, including protection of life, health, the marine environment and property, by using risk analysis and cost-benefit assessment."*

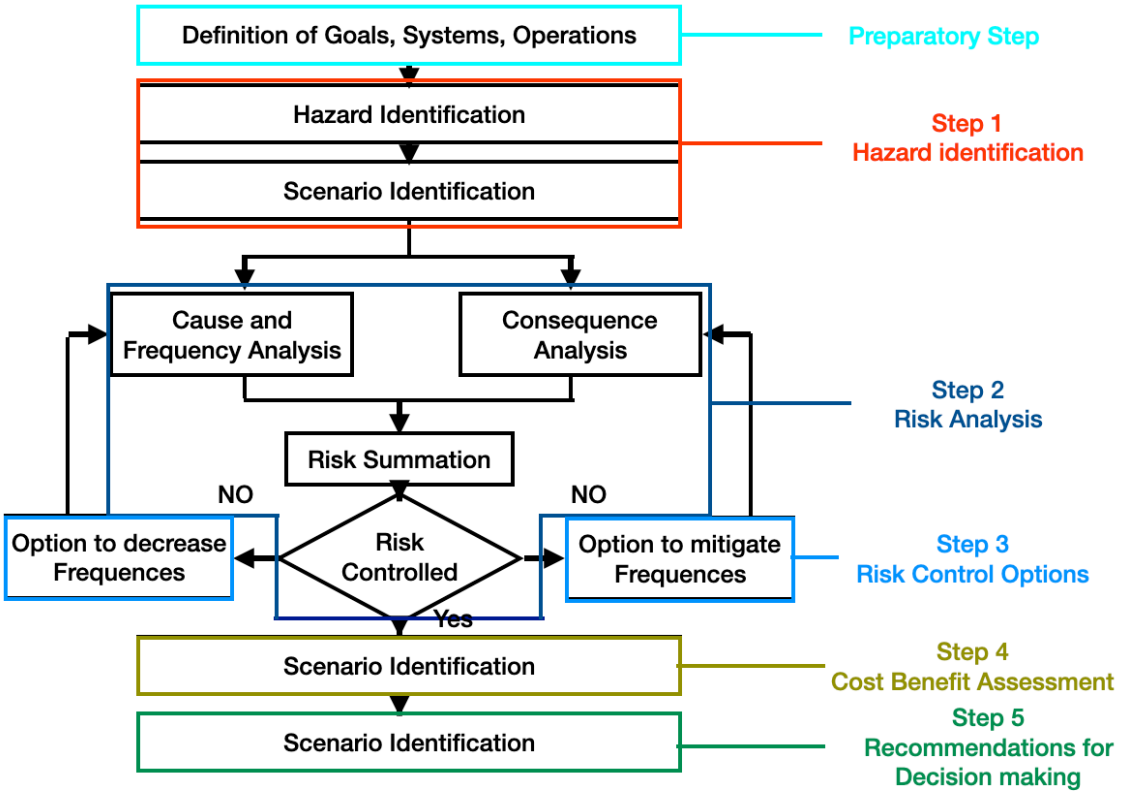


Figure 2-3: FSA Flowchart - Source: International Association of Classification Societies (2005)

Formal Safety Assessment (FSA) follows the rationale of risk assessment techniques and recommends a five-step approach in Figure 2-3, consisting of Hazard Identification (Step 1), Risk Assessment (Step 2), proposing mitigation solutions – that is, Risk Control Option (RCO) in the FSA terminology – (Step 3), performing a Cost-Benefit assessment (Step 4) and, finally providing recommendations for decision making (Step 5).

Per the FSA guidelines, risk is defined as "the combination of the frequency and the severity of the consequence". Originally FSA has been used to address mainly risks to human life. The Guidelines now include provisions to evaluate risks related to environmental risks i.e., related to the prevention of oil spills from ships.

Academic research has suggested using FSA to address various maritime concerns, including ship air emissions (e.g., Kontovas and Psaraftis, 2010; Vanem, 2012) and ship strikes, such as whale-ship collisions (e.g., Sèbe et al., 2019). Furthermore, several

papers have proposed applying FSA to quantify and assess maritime security risks, as seen in the work of Yang et al. (2013) and Yang and Qu (2016).
Elements of the FSA have been used in the novel model proposed by Bolbot et al. (2020) to address cybersecurity, but overall, the applications of FSA to address cybersecurity risks are somewhat limited. As highlighted earlier, the rationale behind most cybersecurity applications - unrelated to the maritime domain, though- is slightly different in that vulnerability assessment plays a significant role (see also Section 2.1).

However, as discussed above, using a traditional safety-based approach to address maritime cybersecurity risks is more complex. There is a need for a new way of thinking to access maritime cybersecurity; for example, Bolbot (2020) and Yang and Qu (2016) argue that novel approaches are needed due to the high uncertainties involved. The latter proposes a novel approach combining a number of techniques such as fuzzy evidential reasoning approach, Bayesian networks and multicriteria analysis methods (Analytic Hierarchy Process and Technique for Order Preference by Similarity to an Ideal Solution).

2.4 Cybersecurity-Related Risk Management Frameworks

In the literature, several cybersecurity-specific frameworks could be found, some generic and others specific to the maritime domain.

2.4.1 IMO Guidelines on Maritime Cyber Risk Management

As already mentioned in the Introduction, the IMO released in July 2017 the ‘Guidelines on Maritime Cyber Risk Management’ (MSC-FAL.1/Circ.3), which supersedes the interim guidelines contained in MSC.1/Circ.1526 published a year earlier in June 2016.

It urges the relevant stakeholders to *"take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping"*.

They provide high-level recommendations on *"maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities"* and are therefore not very specific. For details and guidance related to the developing and implementing of specific management processes, these Guidelines instruct the companies to refer *"to specific Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices"*.

They Guidelines highlight the fact that cybertechnologies have *become "essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment"* and identify the following vulnerable systems: Bridge systems, Cargo handling and management systems; Propulsion and machinery management and power control systems; Access control systems; Passenger servicing and management systems; Passenger facing public networks; Administrative and crew welfare systems; and Communication systems.
There is also a distinction between information technology (IT) and operational technology (OT) systems; the former is considered to focus on the use of data as information, and the latter on the use of these data to control or monitor physical processes.

Effective cyber risk management should, according to the Guidelines, consist of the following function elements, *which "are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework"* as follows:

1. *"Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.*
2. *Protect: Implement risk control processes, measures, and contingency planning to protect against a cyber event and ensure the continuity of shipping operations.*

3. *Detect: Develop and implement activities necessary to detect a cyber event promptly.*
4. *Respond: Develop and implement activities and plans to provide resilience and restore systems necessary for shipping operations or services impaired due to a cyber-event.*
5. *Recover: Identify measures to back up and restore cyber systems necessary for shipping operations impacted by a cyber-event."*

2.4.2 BIMCO-led Guidelines on Cyber Security Onboard Ships

The Baltic and International Maritime Council (BIMCO) is the world's largest international shipping association, with over 1,900 members in around 130 countries representing 60% of the world cargo fleet measured by tonnage.

In February 2016, BIMCO led an industry initiative publishing the first-ever 'Guidelines on Cyber Security onboard Ships'. The consortium included a number of associations such as the Cruise Lines International Association (CLIA), International Chamber of Shipping (ICS), International Association of Dry Cargo Shipowners (INTERCARGO), International Association of Independent Tanker Owners (INTERTANKO), the International Union of Marine Insurance e.V. (IUMI), and shipping companies such as Maersk Line, Wilhelmsen Group COLUMBIA Shipmanagement Ltd and Zodiac Maritime Ltd.

These industry guidelines have been amended several times, with version 2 in July 2017, version 3 in December 2018 and version 4 in Dec 2020. The latest version has been produced and supported by the following: BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), Inter Manager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (SYBASS) and World Shipping Council (WSC).

The guidelines aim to *"assist in the development of a proper cyber risk management strategy in accordance with relevant regulations and best practises on board a ship with a focus on work processes, equipment, training, incident response and recovery management".* The Guidelines argue that while the rapid developments within *"information technology, data availability, the speed of processing and data transfer"* present increased possibilities to optimise operations, reduce costs, improve safety and lead to more sustainable business, these rely on *"increased connectivity often via the internet between servers, IT systems and OT systems*", which, in turn, pose cybersecurity vulnerabilities. Note that these Guidelines divide systems into two: Operational Technology (OT) systems which include hardware and software that monitor and/or control physical devices, processes, and events, and Information Technology (IT) systems, which only include hardware and software, which manages data.

According to the BIMOC-led Guidelines, cyber risk management should:

- *"identify the roles and responsibilities of users, key personnel, and management both ashore and on board*
- *identify the systems, assets, data, and capabilities that, if disrupted, could pose risks to the ship's operations and safety*
- *implement technical and procedural measures to protect against a cyber incident, timely detection of incidents and*
- *ensure continuity of operations through a contingency plan which is regularly exercised."*

The risk management process is illustrated in Figure 2-4.

Figure 2-4: Cyber risk management approach as set out in the BIMCO-led guidelines - Source: BIMCO (2020)

The approach defines clear roles and responsibilities, identifies plans and procedures to raise awareness and provides guidance on incorporating cyber risk management into the company's Safety Management System.

In addition, they list several cyber threats, such as the use of malware and fake websites to exploit unsuspecting visitors and also targeted attacks, such as phishing and Denial of service (DoS) attacks (this type of attack prevents legitimate and authorised users from accessing information, usually by flooding a network with data), provide guidance on how to identify and assess vulnerabilities, and also list a number of protection measures.

2.4.3 ISO/IEC 27001 Standard on Information Technology

ISO/IEC 27001 (ISO, 2022a) is an internationally recognised standard for information security management for businesses to establish, implement, operate, monitor, review, maintain, and continually improve an information security management system (ISMS). ISO 27001 ISMS is an integrated system of policies, procedures, and other controls involving people, processes, and technology for ensuring the security of information assets, which are built on regular risk assessments and technology and vendor neutrality. ISO 27001 is one of the most popular information security standards in the world, and it is recognised as independent accredited certification of the standard. It plays a crucial role in cybersecurity as it provides comprehensive guidelines for managing information security risks. It helps organisations to identify and manage security threats, vulnerabilities, and risks associated with the confidentiality, integrity, and availability of information. By implementing the ISO 27001 standard, organisations can ensure that their information security measures are aligned with best practices and are effective in protecting against cyber threats. The ISO 27001 standard is used by organisations of all sizes and types, including government agencies, financial institutions, healthcare providers, and technology companies. It covers all aspects of information security, from risk assessment and management to incident management and business continuity planning.

2.4.4 United States NIST Framework

NIST Cybersecurity Framework is a set of voluntary guidelines for mitigating organisational cybersecurity risks and is published by the US National Institute of Standards and Technology (NIST). The efforts to develop the framework started in February 2013 with the US President Executive Order (EO) 13636, which ordered NIST to work with stakeholders to develop a voluntary framework based on existing standards, guidelines, and practices. The first version was published in 2014; the latest one (v.1.1) was in published in April 2018. In the US and worldwide, the NIST Cyber Security Framework (CSF) is considered a prevalent best practice for addressing cybersecurity.

The framework builds upon existing standards such as ISO 31000:2009 (see Section 2.3.1), ISO/IEC 27005:2017 (see Section 2.4.3) and NIST Special Publication (SP) 800-398; the latter being US NIST's premier tool for managing information security risk.

The framework was initially developed for critical infrastructure, which is defined as: *"Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters".* However, NIST encourages *"any organization or sector to review and consider the Framework as a helpful tool in managing cybersecurity risks". Its application, especially in the US, has been extensive.*

The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles.

The Framework Core is a set of *"cybersecurity activities, desired outcomes, and applicable references"* that are common across critical (see the note above) infrastructure sectors and consists of 5 concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover; see Figure 2-5. Per the Framework, these Functions, when considered together, provide a high-level, strategic view of the lifecycle of an organisation's management of cybersecurity risk. The Framework Core elements work together as follows:

- *"Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.*
- *Protect – Develop and implement appropriate safeguards to ensure delivery of critical services.*
- *Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.*
- *Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.*

- *Recover – Develop and implement appropriate activities to maintain plans for resilience and to rest."*

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figure 2-5: NIST Framework Core Functions, Categories and Subcategories - Source: NIST (2023)

The above five elements provide detailed guidance for developing individual, organisational Profiles. Then, Framework Profiles can be used to describe the current state and/or the desired target state of specific cybersecurity activities. Current Profiles indicate the outcomes that the organisation is currently achieving, while Target Profiles indicate the outcomes needed to achieve the desired cybersecurity risk management goals. Comparing these Profiles may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps to fulfil a given Category or Subcategory of the Framework Core (see Figure 2-5) can aid in setting priorities considering the organisation's business needs and its risk management processes.

2.4.5 ENISA Cyber Risk Management for Ports

ENISA (European Union Agency for Cybersecurity) was established in 2004 to task with promoting a uniform and robust level of cybersecurity throughout the member states of the European Union (EU). ENISA's cyber risk management framework is targeted port authorities, port facilities / terminal operators, and other entities operating within ports to o pinpoint effective cybersecurity strategies for managing cyber risks, as well as to conduct a self-assessment of cybersecurity maturity that will aid in the efficient allocation of cybersecurity budgets and the establishment of priorities.

Figure 2-6: ENISA cyber risk management phases - Source: ENISA (2020)

The ENISA cyber risk management approach consists of four phases, which are designed to offer practical guidelines for managing cyber risk that can be applied to any existing or desired framework or methodology used by a port operator. The first three phases align with the risk assessment methodology's minimum requirements detailed in the ISPS Code, Regulation 725/2004 and Annex I of Directive 2005/65. The fourth phase proposes a cybersecurity maturity self-assessment model that enables port operators to evaluate their security measures, prioritise investment of resources for improvement and lay the groundwork for building a programmatic foundation to achieve organisational cybersecurity maturity. It is important to note that this approach does not aim to provide a comprehensive methodology for cyber risk management but rather offer actionable guidance for managing cyber risk in the context of port operations. In Figure 2-6, the four phases are:

- *Phase 1: Identifying cyber-related assets and services (ISPS Code Section 15.5.1: Identification and evaluation of essential assets and infrastructure it is important to protect)*
- *Phase 2: Identifying and evaluating cyber-related risks (ISPS Code Section 15.5.2: Identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures, ISPS Code Section 15.5.4: Identification of weaknesses, including human factors in the infrastructure, policies and procedures)*
- *Phase 3: Identifying security measures (ISPS Code Section 15.5.3: Identification, selection and prioritization of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability)*
- *Phase 4: Assessing cybersecurity maturity.*

2.4.6 Comparison

In summary, IMO and BIMCO focus primarily on the maritime industry, while ISO/IEC, NIST, and ENISA offer a comprehensive framework applicable to various sectors. Each organisation adopts a risk-based approach, but the specific requirements and recommendations may vary. Maritime organisations should adopt a holistic approach by integrating elements from these guidelines that align with their operational context and needs. Additionally, given the evolving landscape of cybersecurity threats and best practices, it is crucial to stay updated with the latest revisions and additions to these guidelines. Furthermore, ongoing cybersecurity research in academia is essential.

2.5 Other Relevant IMO Literature

Besides the IMO literature mentioned earlier (FSA, IMO Guidelines and BIMCO-led), there are also some relevant IMO Codes; the interested reader could refer to these publications for more.

2.5.1 ISPS Code

International Ship and Port Facility Security Code (ISPS) were discussed to enhance maritime assets such as ship and port facilities, designed in response to protect the

maritime assets from threats after the 9/11 attack by IMO in 2002. The Code was bought into force on July 1st, 2004. Its objectives are the following:

- *"to establish an international framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade;*
- *to establish the respective roles and responsibilities of the Contracting Governments, Government agencies, local administrations and the shipping and port industries at the national and international level for ensuring maritime security;*
- *to ensure the early and efficient collection and exchange of security-related information;*
- *to provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels; and*
- *to ensure confidence that adequate and proportionate maritime security measures are in place."*

2.5.2 ISM Code

The International Safety Management (ISM) code is the IMO Code *"for the Safe Operation of Ships and for Pollution Prevention adopted by Organization by resolution A.741(18), as may be amended by the Organization, provided that such amendments are adopted, brought into force and take effect in accordance with the provisions of article VII of the present Convention concerning the amendment procedures applicable."*

This Code provides international standards for shipping operations, management of safety and pollution prevention. It was adopted in 1993 by resolution A.741(18) in its present form, and in 1994 amendments to the SOLAS Convention, it was stated mandatory into force on 1st July 1998.

"Safety management objectives of the company should:

- *Provide safe practices in ship operation and a safe working environment;*
- *Assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards; and*

- *Continuously improve safety management skills of personnel ashore and aboard ships, including preparing for emergencies related to both safety and environmental protection.*

The safety management system should ensure the following:

- *Compliance with mandatory rules and regulations; and*
- *That applicable codes, guidelines and standards recommended by the Organization, Administrations, classification societies and maritime industry organization are taken into account."*

According to the ISM Code, which was reinforced by the IMO's MSC.428(98), ship owners and managers are required to assess cyber risk and implement measures relevant to their safety management systems until the first Document of Compliance (DOC) is issued after January 1, 2021.

2.6 Classification Societies-led Related Literature.

2.6.1 Det Norske Veritas (DNV, previously known as DNV-GL)

Det Norske Verutas (DNV) is one of the classification societies in the world and a recognised advisor for the maritime industry. DNV published cybersecurity recommended practice DNVGL-RP-G496 titled 'Cyber security resilience management for ships and mobile offshore units in operation' in 2016 (DNV, 2016). It aims to suggest further practical guideline-based BIMCO and IMO guidelines for cybersecurity in maritime organisations that want to assess cybersecurity risk, improve cybersecurity and implement information cyber security management (CSM) systems. Figure 2-7 illustrates the assessment Step of the process; note here that this document presents an interesting approach to assessing the risks, namely the bowtie method, more on which in Chapter 6.

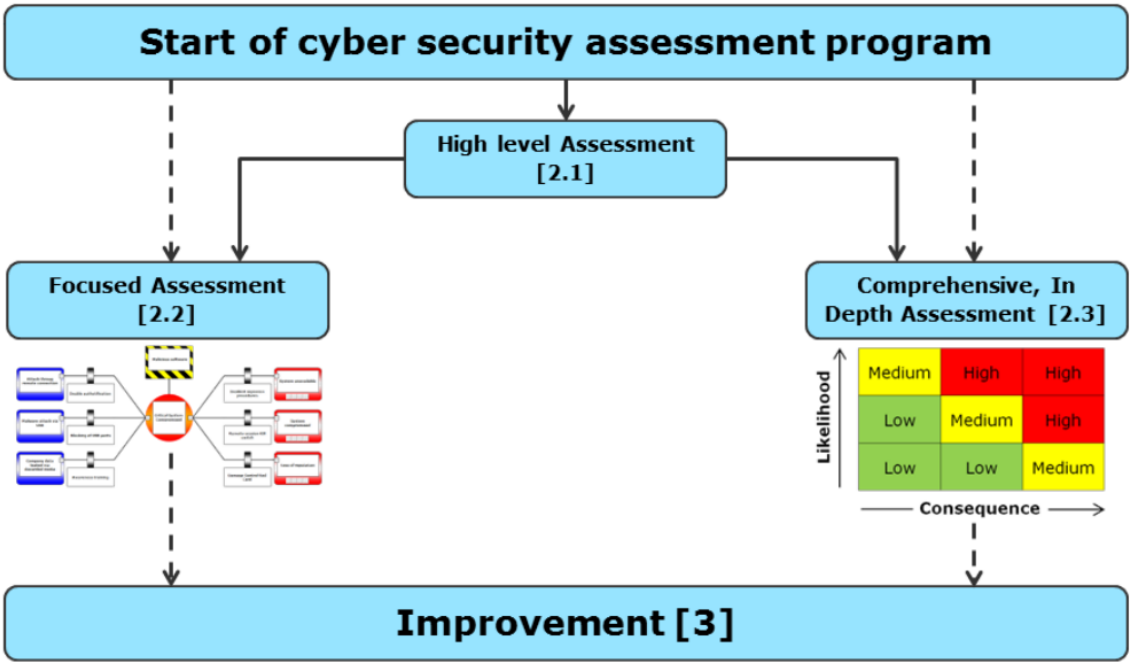


Figure 2-7: Assessment sequence - Source: DNV (2016)

This recommended practice categorises cyber security threats to onshore and vessel systems within the following:

- *"Unintentional infections / non-targeted threats:*
  - *Software infections stemming from malicious malware or ransomware: Spreading via unsuspecting and insufficiently trained users in combination with unsecured internet access or insufficiently protected use of portable storage devices like USB sticks, the infection thrives through automated replication aimed at infecting as many systems as possible. These non-targeted threats typically exploit known vulnerabilities in standard systems and networks.*
  - *Unintentional weaknesses in software:*

    They typically stem from misconfiguration of equipment and software as well as from software design or updates containing undetected weaknesses due to insufficient verification and validation of the software.
- *Intended/targeted threats:*
  - *External attackers: Hackers, "hacktivists", as well as criminal attackers employing a wide range of attack techniques and malicious software infections. These*

include phishing, social engineering, exploitation of weaknesses in control systems, user authentication or lack of network segregation.

- *Insider threats: Originating from disgruntled employees or from employees that intend to sell or otherwise misuse data or system access. Their ability to circumvent physical access controls and their in-depth knowledge of the systems makes them particularly difficult to defend against."*

According to this guideline, there are three steps for cybersecurity resilience in following:

"ASSESSMENT: A systematic assessment is the foundation of cyber security improvements. Due to the potentially substantial cost of conducting detailed assessments across all systems, data sets and organisational units, this RP recon and in mends three different assessment levels, each serving a different need and using tailored methodologies.

IMPROVEMENT: Most activities required to improve cyber security can be directly derived from the above-described assessments.

VERIFICATION and VALIDATION: To obtain assurance of the achieved cyber security and to demonstrate compliance and progress towards external stakeholders and the company's board, cyber security resilience can be validated and verified."

2.6.2 Lloyds Register (LR)

Lloyd's Register is the first marine classification society, from 260 years ago, and a global specialised services company to improve the safety of vessel in engineering and technology for the maritime industry. They published three cybersecurity guidance notes in 2016, *'Cyber-Enabled Ships—Deploying Information and Communications Technology in Shipping'*, '*Cyber-Enabled Ships—Ship Right Procedure—Autonomous Ships'*, and *'Cyber-Enabled Ships—Type Approval of Cyber-Enabled Systems Components'.* They are based on IMO Resolution MSC.428(98) and IMO Guidance MSC-FAL.1/Circ.3. They cover implementing IT and OT systems for assets in the maritime industry and autonomous ships. Furthermore, Cyber-enabled components of vessel IT and OT systems are contented with LR Cyber Security Framework (CSF) for the Marine and Offshore sector.

2.6.3 American Bureau of Shipping (ABS)

The American Bureau of Shipping (ABS) is an American maritime classification society founded in 1862, providing classification services for marine and offshore assets. ABS published the '*Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations'* in 2016, and four more cybersecurity-related documents; '*Guidance Notes on Data Integrity for Marine and Offshore Operations', 'Guide for Software Systems Verification' and 'Guidance Notes on Software Provider Conformity Program'* in 2016, and '*Guide for Cybersecurity Implementation for the Marine and Offshore Industries'* in 2018. Those published documents apply to the shipping company, operator, and owner. They provide well-constructed guidelines for measures of operational and technical aspects of cyber security. As well as providing guidance on data integrity, these documents highlight mitigation measures applied to IT and OT systems for maritime assets.

2.6.4 Korean Register

Korean Register (KR) is the only international vessel inspection agency in Korea, which was established to promote safety and technology related to shipbuilding and maritime affairs in 1960; as well as it is one of the members of the International Association of Classification Societies (IACS). They published marine cybersecurity guidelines established to strengthen safety against internal and external cyber threats for IT technologies and services introduced and operated by onboards and offshores in 2019. It is based on ISO 27001, NIST, IEC 62443, etc., which are internationally widely used cyber security international standards. It implements recommendations on IMO cyber risk management, as well as international IMO, BIMCO, Digital Container Shipping Association (DCSA), etc. (see Figure 2-8). It is designed based on the cyber risk management framework recommended by the maritime industry and identifies cyber threats.

According to this guideline, in addition to the IT system onboard ship, the OT system related to ship functions, such as power generation and distribution, steering, navigation, communication etc., also needs cyber security.

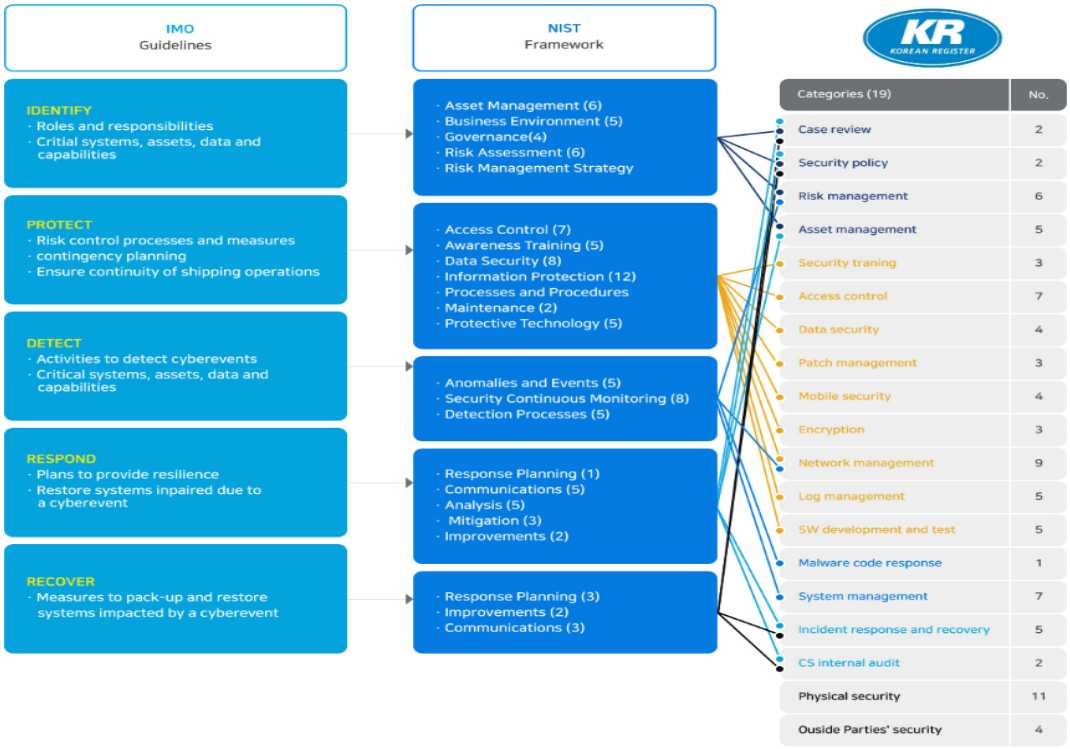


Figure 2-8: KR's Cyber Risk Management Framework - Source: Korean Register website (2023)

2.6.5 Japanese Ship Classification Society

The Japanese ship classification society Class NK published 'Cyber Security Management Systems for Ships' for applying cybersecurity elements for ships in 2019 (Class NK, 2019). Furthermore, 'Guidelines for Designing Cyber Security Management Systems for Ships' was published in 2020. They deal with the cybersecurity management of IT and OT systems for maritime assets and the implementation of operational and technical measures against cyber threats for IT and OT systems on ships.

2.6.6 Indian Register of Shipping (IRClass)

The Indian Register of Shipping (IRClass) published 'Guidelines on Maritime Cyber Safety' (IRS-G-SAF-02-2017) in 2017 (IRClass, 2017) "*to provide requirements for evaluating and managing the Cyber Risk of Ships. For these Guidelines, Ship includes mobile offshore units. If requested by the Owner, IRS can verify and certify the associated shore-based support facilities, as indicated in Section 2 of these Guidelines".* Furthermore, they published 'Guidelines on Certification of Software for Computer Based Control Systems'

(IRS-G-DES-01—2019) in 2019 (IRClass, 2019) for the quality assurance certification requirements for computer-based control system software and on-board application.

2.7 Other Industry-led Related Literature

In the realm of industries, the maritime industry has relatively recently grappled with cybersecurity challenges. Notably, sectors like finance, military information, government agencies, and IT technologies have swiftly integrated cybersecurity measures, leaving the maritime industry facing security management issues that are central to its operations.

Diverging from these industrial sectors, the unique devices employed in ships, inherent to the cybersecurity landscape of the maritime industry, merit attention. The imperative for a comprehensive cybersecurity risk management framework has become a focal point, encompassing not only ship operation safety components like AIS, ECDIS, and GPS but also extending to port facilities and the systems of shipping line companies. This emerging discourse underscores the pressing need for an all-encompassing approach to address cybersecurity vulnerabilities within the shipping industry and its interconnected domains.

2.7.1 IAPH Cybersecurity Guidelines for Ports and Port Facilities

The International Association of Ports and Harbours (IAPH) recently launched its Cybersecurity Guidelines for Ports and Port Facilities in 2021. IAPH was established in 1955 as a non-profitable global alliance, with 170 ports and 140 port-related organisations in 90 countries in the world at present.

IAPH guideline was designed to support the world's port and port facility community in a manner consistent with IMO's Guidelines (MSCFAL.1/Circ.3, July 5, 201710). Cybersecurity guidelines provided by the IMO are non-prescriptive guidance on improving the cybersecurity resilience of the shipping industry in the face of current and emerging cyber threats. It aims *“to assist ports and port facilities to establish the true financial, commercial & operational impact of a cyber-attack.”*

2.7.2 Flag States

The United States Coast Guard (USCG)

The United States Coast Guard (USCG) is the flag states organisation of the United States, with the purpose of maritime security, search and rescue, and law enforcement service. They released an updated 'Cyber Strategy Outlook' in 2021 to address the latest threat of cyberattacks against significant maritime systems and essential facilities to the Nation's economy and security.

The outlooks content USCG actions in response to this Outlook are organised into three lines of effort:

- *"(1)Defend and Operate the Enterprise Mission Platform;*
- *(2) Protect the Marine Transportation System; and*
- *(3) Operate In and Through Cyberspace. "*

According to the Outlooks, to achieve unity of effort, these efforts will be based on developing and maintaining a skilled workforce, intelligence-driven operations, and international and domestic partnerships.

The Maritime and Coastguard Agency (MCA)

The Maritime and Coastguard and Agency (MCA), which is The United Kingdom's organisation, released 'Incorporation of Cyber Security Measures within Safety Management Systems' (MIN 647 (M)) in 2021. It informs the industry that cyber security should be incorporated into the management procedures of UK boards, as well as it regulates vessels where required and advises other operators on how to detect and address cyber security threats.

2.8 Insurance Companies

It is the international Protection and indemnity insurance club (P&I), to cover damages and loss as well as costs and expenses, which are related to shipping accidents. Recently, P&I clubs have dealt with cyberattacks in various ways. Therefore, maritime asset

insurance includes the Institute Cyber Attack Exclusion Clause (CL 380) 10/11/2003. Computer equipment and systems are covered under most marine insurance policies in CL 380; in contrast, it does not cover losses, damages, or liabilities resulting from using systems or equipment for aggressive or nefarious purposes.

The North of England P&I Association suggests following IMO Guidance MSC-FAL.1/Circ.3, IMO Resolution MSC.428(98) and the BIMCO Guidelines on Cyber Security Onboard Ships (BIMCO,2020). Furthermore, they published several documents and circulars such as 'Loss Prevention Briefing: Cyber Risks in Shipping' (The North of England P&I Association, 2017), 'Circular 2020/02: Cyber Security: Kick Start—New Member Benefit for Cyber Security Compliance' (The North of England P&I Association , 2020), Circular 2021/06: Class War Risks—Renewals 2021/2022(The North of England P&I Association, 2021), to protect customers' assets from the cyber security threats, and OT vulnerabilities faced by the maritime industry.

The Standard Club is a mutual insurer that provides protection and indemnity insurance to shipowners and operators. In response to the growing threat of cyberattacks on the maritime industry, the Standard Club has developed a set of guidelines for managing cyber risks in the maritime sector. These guidelines are known as the Maritime Cyber Risk Management Guidelines.

The Maritime Cyber Risk Management Guidelines provide a framework for identifying, assessing, and managing cyber risks in the maritime industry. The guidelines are designed to be flexible and scalable so that they can be applied to vessels of all sizes and types, as well as to shore-based operations. The guidelines cover a range of topics, including:

- *"Cyber risk governance: This section covers the roles and responsibilities of individuals and organizations in managing cyber risks, as well as the need for a cyber risk management plan.*
- *Risk identification and assessment: This section outlines the process for identifying and assessing cyber risks, including the use of risk assessments, vulnerability assessments, and penetration testing.*

- *Risk mitigation: This section covers the various ways in which cyber risks can be mitigated, including the use of firewalls, anti-virus software, and intrusion detection systems.*
- *Incident response: This section outlines the steps that should be taken in the event of a cyber incident, including the need for a response plan and incident reporting.*
- *Training and awareness: This section covers the importance of training and awareness programs for all individuals involved in the maritime industry, including crew members, shore-based staff, and third-party contractors".*

The Standard Club's Maritime Cyber Risk Management Guidelines are an important tool for the maritime industry to manage cyber risks and protect against cyberattacks.

2.9 Aviation Industry

As technology advances rapidly, aircraft systems are increasingly integrating more technological elements, either to streamline tasks or enhance services for passengers. At the same time, concerns about cybersecurity risks have been present since the early 2000s, however, the primary challenges confronted by cybersecurity in aviation include insufficient resources, budgetary limitations, and a shortage of expertise in the field of cybersecurity. The quantity of cyber threats is consistently escalating each year, accompanied by a corresponding increase in the sophistication of these threats (Lykou et al., 2018; Kagalwalla and Churi, 2019).

Therefore, the International Civil Aviation Organization (ICAO) prompted to formulate a cybersecurity strategy for the aviation industry (Abeyratne, 2016; Filinovych and Hu). This strategic response emerged as the civil aviation sector increasingly relied on technology. Over time, ICAO's initiatives and discussions expanded to encompass the broader air transport sector. Therefore, ICAO complied NIST's 'Framework for National Infrastructure Cybersecurity', which has core function 'Identify, Protect, Detect, Respond, and Recover' (see Section 2.4.4 in detail) to set high-level standards for

aviation security. Published in 2019, ICAO's cybersecurity strategy (ICAO, 2019a) is aligned with other cyber-related initiatives and harmonised with safety and security management provisions (Stastny and Stoica, 2022). The strategy is structured around seven pillars, consisting of principles, measures, and actions:

- *"International cooperation;*
- *Governance;*
- *Effective legislation and regulations;*
- *Cybersecurity policy;*
- *Information sharing;*
- *Incident management and emergency planning; and*
- *Capacity building, training and cybersecurity culture".*

The significance of addressing cybersecurity in civil aviation was underscored by the adoption of three ICAO Assembly resolutions: Resolution A39-19 (ICAO, 2016), succeeded in 2019 by Resolution A40-10 (ICAO, 2019b), and in 2022 by Resolution A41-19 (ICAO, 2022). These resolutions reinforce the commitment to enhancing cybersecurity measures within the aviation industry.

Furthermore, other international aviation organisations promoted cybersecurity guideline and policy.

The European Union, via the European Parliament, enacted Regulation (EU) 2018/1139, which established a new Basic Regulation for civil aviation. This regulation includes an updated mandate for the European Union Aviation Safety Agency (EASA), designating the agency as a key player in enforcing EU cybersecurity regulations in aviation. EASA is tasked with managing interdependencies among various aviation safety domains, cybersecurity, and other technical aspects of aviation regulations (Lekota and Coetzee, 2021). Federal Aviation Administration (FAA) in the U.S has instituted a policy to provide guidance to airplane certification offices regarding the application of special conditions. According to this policy, special conditions are issued for e-enabled airplane systems that directly link to non-governmental external services and networks, with a specific focus on airplane systems classified as "major" or higher in terms of criticality. Examples

of such networks encompass gatelink networks, public networks, wireless airplane sensors and sensor networks, cellular networks, and portable electronic devices like electronic flight bags (Pyzynski and Balcerzak, 2021; Ukwandu et al., 2022).

The aviation sector has initiated the development of cybersecurity strategies and risk management, but there is room for improvement in addressing emerging threats. Similarly, the maritime industry is also in the process of enhancing its cybersecurity risk management practices. Both industries recognise the imperative to continually refine and strengthen their approaches to effectively mitigate evolving cyber threats.

2.10 Financial Industry

In the 1990s, cybersecurity concerns emerged in the finance industry as advancing technology increased the vulnerability of financial data. In response, entities like the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the National Institute of Standards and Technology (NIST) developed comprehensive cybersecurity standards. Financial institutions widely adopted these standards, customising them to meet their specific needs.

Some financial cybersecurity framework has been proposed. For instance, Saudi Arabian Monetary Authority (SAMA) established 'Cyber Security Framework Ver1' to effectively identify and address risks related to cybersecurity in 2017 (SAMA,2017). The framework is grounded in the requirements outlined by SAMA and aligns with established industry cybersecurity standards, including but not limited to NIST, ISO, Information Security Forum (ISF), Basel accords, and the Payment Card Industry Security Standards Council (PCI SSC).

It has four domains;

- *"Cyber Security Leadership and Governance.*
- *Cyber Security Risk Management and Compliance.*
- *Cyber Security Operations and Technology.*
- *Third Party Cyber Security."*

Figure 2-9 illustrates the comprehensive structure of it, delineating the various cyber security domains and subdomains. It also includes references to the corresponding sections within the framework.

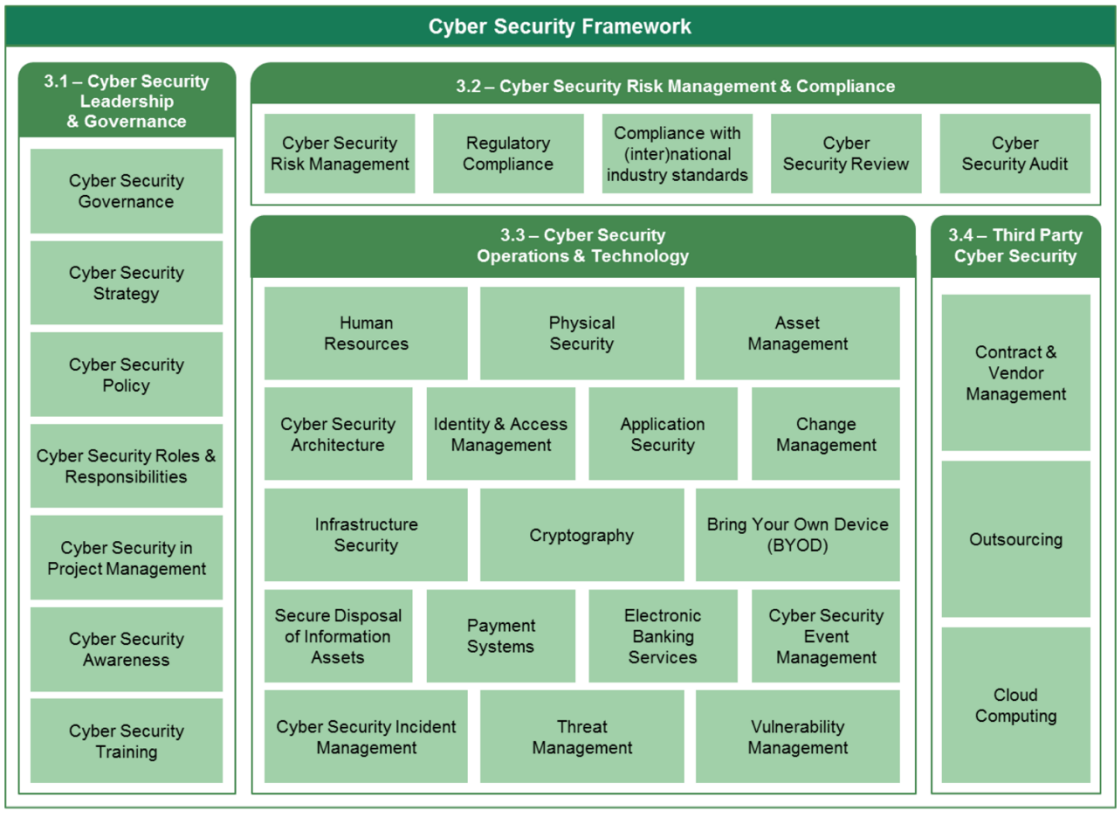


Figure 2-9: Cyber Security Framework of SAMA – Source: SAMA (2017).

Matsikidze and Kyobe (2020) introduced a conceptual cybersecurity framework model for financial institutions. The model is designed to enhance the effectiveness of cyber security audits, ultimately aiming to improve cyber safety within the financial sector. The conceptual model is based on established frameworks such as The Control Objectives for Information and Related Technologies (COBIT), ISO 27000 standards, and the NIST cybersecurity framework model. It comprises IT risk assessment as a dependent

construct, while individual attributes and internal factors serve as independent constructs. This configuration demonstrates that both internal factors and individual attributes play a crucial role in facilitating the efficient auditing of cyber security. Figure 2-10 illustrates the conceptual model.

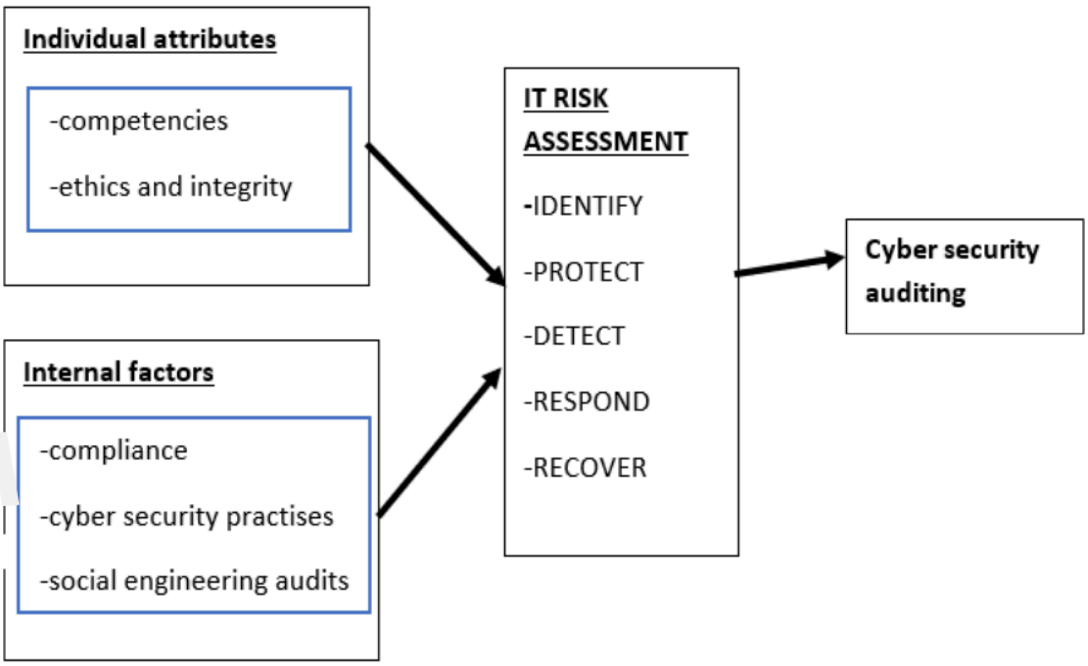


Figure 2-10: Cyber security framework for auditing in financial institution – Source: Matsikidze and Kyobe (2020)

In other hand, in the mid-2000s, the Payment Card Industry Security Standards Council (PCI SSC) introduced the Payment Card Industry Data Security Standard (PCI DSS), specifically designed to protect credit cardholder data during transactions (Morse et al, 2008). This standard became a crucial framework for cybersecurity in the finance sector. The NIST Cybersecurity Framework, launched in 2014, gained widespread adoption in various industries, including finance (NIST, 2014). This framework provides a flexible strategy for managing cybersecurity risks, covering functions such as Identify, Protect, Detect, Respond, and Recover.

Global regulators have intensified their supervision of cybersecurity practices within the finance sector by conducting examinations and setting specific requirements. Guidelines

have been issued to guarantee the implementation of strong cybersecurity measures by financial institutions (Mishra et al., 2022). Due to the dynamic nature of cybersecurity threats, it has become crucial to update and revise guidelines continually. Regulatory bodies and industry organisations consistently review and enhance standards to address emerging threats and technological advancements (Uddin et al., 2020). The finance industry has adopted cutting-edge technologies such as artificial intelligence, blockchain, and cloud computing (Smith and Dhilion, 2020). As a result, cybersecurity guidelines in the finance industry have evolved to address the distinct risks associated with these technologies, ensuring a comprehensive and adaptable security approach (Smith and Dhilion, 2020; Mishra et al., 2022).

Cybersecurity varies based on the structures of the financial and maritime industries. The financial sector prioritises data security. As the industry has evolved, cybersecurity has gained significance in safeguarding personal information, including activities such as personal financial transactions and cryptocurrency. Although it is a distinct industry, we acknowledge the necessity of consistently enhancing and fortifying our approach to mitigate emerging cyber threats effectively through the implementation of computerised digitalisation.

2.11 Academic Literature

A literature review critically analyses published academic literature, mainly peer-reviewed papers and books, on a specific topic. This is usually the first thing students do at the beginning of their studies. At a very early stage of the research, it was clear that for the specific topic –i.e., maritime cybersecurity– the grey literature is much more comprehensive and critical for the industry as a policy issue is dealt in this research.

Usually, the grey literature can be challenging to search and retrieve, but this is not the case for our topic; the IMO regulations are widely available, and there are all these rules and guidelines that were presented in the previous Sections. In our case, it has been actually much more difficult to find relevant academic papers due to the number of

different keywords used in addressing the specific topic. In the below, the approach to reviewing the literature and our findings is presented.

As a first step, the relevant literature surveys were identified. A handful of literature review papers have been identified.

Drummond and Machado (2021) present the results of a systematic literature review related to cybersecurity risk management but focus on ports only. The analysis is based on search results on IEEE Xplore, Science Direct and Scopus. Data extraction has shown that the digital library with the most results was Scopus, which returned 62.4% of the studies, while the IEEE Digital Library retrieved only 16.1% of the results. The following string has been used to extract the relevant data for their analysis from Scopus:

> *TITLE-ABS-KEY ((”cybersecurity” OR ”cyber security” OR ”cybersecurity assets” OR ”cybersecurity risks”) AND (”management” OR ”address” OR ”assessment” OR ”evaluation” OR ”valuation”) AND (”framework” OR ”approach” OR ”method” OR ”model” OR ”process” OR ”strategy” OR ”study”) AND (”port” OR ”maritime port” OR ”seaport” OR ”port infrastructure” OR ”port systems”)) AND (LIMIT-TO (DOCTYPE, ”ar”) OR LIMIT-TO (DOCTYPE, ”cp”)) AND (LIMIT-TO(LAN-GUAGE, ”English”))*

A literature review by Farah et al. (2022) entitled Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends attempts to comprehensively assess cybersecurity frameworks and classify cyberattacks within the maritime industry. Data were extracted from three scientific databases (Science Direct, Springer and IEEE) using the keywords: "Maritime”, “Cyber-attack” + “Maritime” and, “Cyber-attack” + “Port."

Progoulakis et al. (2021) present the relevant standards, guidelines and number of publications mainly belonging to the grey area. Risk analysis and assessment methods are the main focus of their survey. No bibliometric analysis is presented.

Bolbot et al. (2022) focused on the development and application of cybersecurity risk assessment techniques, as well as the design of monitoring and intrusion detection tools

for cyberattacks in maritime systems. They utilised the Preferred Reporting Items for Systematic Reviews and Meta-analysis (PRISMA) methodology to review maritime cybersecurity studies, address methodological challenges, and suggest research directions. This effort aimed to facilitate the development of research proposals, innovative methodologies, and technical solutions. Data is from Scopus and using keywords: "maritime cybersecurity", "maritime cyber security", "ship cybersecurity", "ship cyber security", "port cybersecurity', and "port cyber security".

In the below, the results of bibliometric analysis are presented. Note that there is no intention to duplicate the work performed by other researchers. Therefore, interested readers are referred to the comprehensive surveys on maritime cybersecurity presented by Progoulakis et al. (2021) and Bolbot et al. (2022).

2.11.1 Bibliometric Analysis

This bibliometric analysis was conducted to identify key academic literature and gain valuable insights. The analysis was updated and performed in mid-May 2023.

While a multitude of software tools are available to facilitate bibliometric analysis, it is notable that not all of them encompass a comprehensive and recommended workflow for scholars (Aria and Cuccurullo, 2017). Among the well-recognised tools in this domain are Citespace (Chen, 2006) and VOSviewer (van Eck and Waltman, 2010). Both of these are Java-based applications, freely accessible, designed to visualise and analyse trends and patterns within scientific literature. These tools specifically excel in rendering bibliometric maps in a visually comprehensible manner, making them particularly valuable for the interpretation of extensive bibliometric data maps.

However, to perform this task, 'Bibliometrix' (a well-known R statistical language tool) has been utilised; see Aria and Cuccurullo (2017) for more. This package is scripted in the R language, an open-source environment and ecosystem. The presence of robust and efficient statistical algorithms, access to top-tier numerical procedures, and the

inclusion of integrated data visualisation tools are key factors that make R a preferable choice over other programming languages for scientific computations (Aria and Cuccurullo, 2017; Munim et al., 2020).

Data has been extracted from Scopus; out of all databases supported by the specific tool, this is the one that indexes the most documents, which is in line with Drummond and Machado (2021). The Scopus website states that it currently indexes approximately 87 million documents. The most important parameter in a bibliometric analysis, especially the software-based ones, is the string used to extract the documents to be further analysed. Based on the literature survey papers and our own detailed investigation, the following strings have been considered; see Table 2-3 for the number of documents returned from each search. Note that documents where the search terms appear adjacent to each other, are returned when enclosing search terms within a double quotation. In addition, "cyber security" and "cyber-security" return the same results as the hyphen is ignored.

Table 2-3: Bibliometric analysis – Search string

Doc. #	SCOPUS Search string
569	TITLE-ABS-KEY ((“cybersecurity” OR “cyber security”) AND (“maritime” OR “port" OR "ship"))
395	**TITLE-ABS-KEY ((cybersecurity OR (cyber AND security)) AND (maritime OR shipping))**
360	TITLE-ABS-KEY ((cybersecurity OR (cyber AND security) OR "cyber security") AND maritime) TITLE-ABS-KEY ((cybersecurity OR (cyber AND security)) AND maritime)
342	TITLE-ABS-KEY (("cybersecurity" OR "cyber security") AND ("maritime" OR "ship"))
304	TITLE-ABS-KEY ((cyber AND security) AND maritime)
319	TITLE-ABS-KEY (("cybersecurity" OR "cyber security") AND ("maritime" OR "marine"))
272	TITLE-ABS-KEY (("cybersecurity" OR "cyber security") AND "maritime")
161	TITLE-ABS-KEY (cyber AND risk AND maritime)
129	TITLE-ABS-KEY (cyber AND risk AND maritime AND security)

In the end, the following string was obtained:

TITLE-ABS-KEY ((cybersecurity OR (cyber AND security)) AND (maritime OR shipping))

Note that searching for the string “cyber AND security” the results will include documents where these two terms are adjacent with, the latter being a subset of the former. The keywords are to be found in the document title, abstract or keywords. Searching within other fields (such as the funder, affiliation, references, or, obviously, ALL fields) is not recommended.

In addition, the first string was rejected as using the word ‘port’ is a bit tricky; in computing, the word (computer) port is very common word and can refer to a physical connection between a computer and another internal or external device (e.g., USB port) or a virtual one such as the number assigned to a server application in an IP network. Same for the term ‘ship’ that might refer to the act of shipping (i.e., sending) goods/cargo; see also comment below.

It should be noted here that the primary aim of the literature review was to identify papers related to the management of cybersecurity risk. However, a wider search could provide us with a larger dataset and help us better understand the domain. It would also help overcome the fact that the risk-related vocabulary is a bit confusing (see also definitions in Section 2.1), and terms like 'risk', 'hazard', 'vulnerability' and 'threat' might refer to the same thing; relevant to risk management documents might include terms such as 'management', 'assessment', 'analysis', 'identification', 'treatment' etc.

The first step was, therefore, to perform a search using the selected string on Scopus. Although this could be the complete search relevant to our work, it has become apparent that some recent papers, such as Tusher et al. (2022), were not included in the results -at least at the time of our search- although its outlet, i.e., the 'WMU Journal of Maritime Affairs' is indexed by Scopus. This document is included in the SCOPUS 'Secondary documents' search results; this is based on the list of documents that have been extracted from a Scopus document reference list but are not directly available in

the indexed literature and its full bibliographical details -at least in the way to be compatible with the 'Bibliometrix' R package- cannot be extracted and cannot, therefore, be included in the bibliometric analysis. The same is true for other documents, for example, those published in conference proceedings that Scopus does not index.

These findings reveal a need for more bibliometric analysis and, in fact, for any analysis using software, and there is room for improvement in identifying the relevant source documents. Another inherent deficiency is that some documents might, for a number of reasons, might not be relevant; in our case, the term 'shipping' could refer to the act or business of a person that ships, i.e., send goods/cargo by any transport means. There is, therefore, the need to manually check the search results and exclude documents that do not appear to be relevant; this involves the risk of human error, though.

2.11.2 Bibliometric Analysis: Main Results

Per the above, after extracting the results (a list of 395 documents -note here that there are also 290 documents that appear as 'secondary' documents, many of which were not relevant), several documents that were not relevant have been manually excluded. The final dataset includes n=207 documents. Full bibliographical data for each document have been exported to be used in the analysis.

The dataset has then been analysed, and the following summarises the results reported by using the 'Bibliometrix' tool; the entire process is visualised in Figure 2-11.

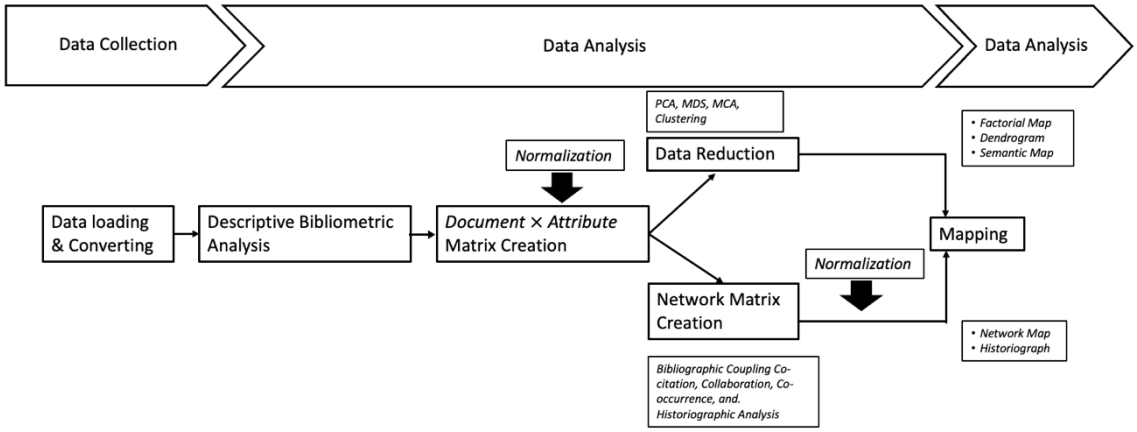


Figure 2-11: 'Bibliometrix' and the recommended science mapping workflow - Source: Aria and Cuccurullo (2017)

Bibliometrics is mainly known for quantifying scientific production and measuring its quality and impact. However, it can be useful for displaying and analysing the intellectual, conceptual, and social structures of research as well as their evolution and dynamic aspects. The descriptive analysis provides useful insights such as on the annual research development, the productive authors, papers, countries, and most relevant keywords.

Documents Analysed

To begin with, regarding the publishing outlets, 207 documents have been analysed; almost half of them (94 docs) are journal papers, and there is also an equal number of documents (another 96 papers) published in conference proceedings.

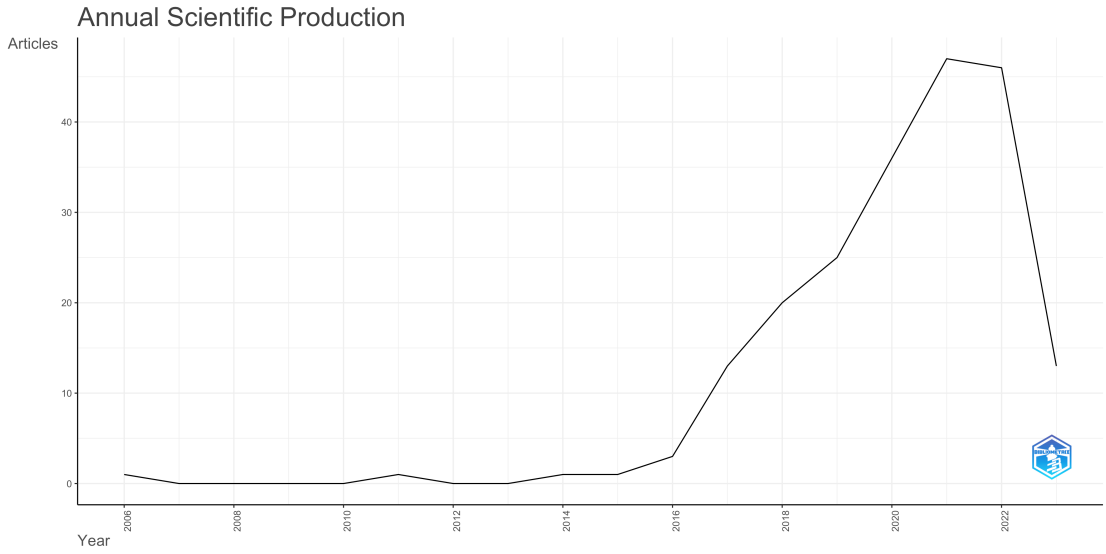


Figure 2-12: Annual Scientific Production (No of articles) - Source: Author's analysis using Bibliometrix

As illustrated in Figure 2-12, which presents the number of papers published per year, there has been an increased engagement with the topic after 2016, with 20 documents published in 2018, 25 in 2019, 36 in 2020, 47 in 2021, 46 in 2022 and 13 until mid-May 2023.

The most relevant outlets are the following: International Journal on Marine Navigation and Safety of Sea Transportation (TRANSNAV) (10), Journal of Marine Science and Engineering (9) and Lecture Notes in Computer Science (7).

Most citations though (based on the reference lists) are to papers published in Journal of Marine Science and Engineering (48), TRANSNAV (40) and Journal of Navigation (37).

Most Cited Papers

Citation counts are often used to measure the impact or influence of academic work in the field. Although this might not always be the case, this analysis will provide a starting point for a more detailed examination of the relevant literature. It could also help identify the important areas of research and methods utilised. Table 2-3 below presents the most cited papers based on the total citations (TC) that an article in the dataset has received from documents indexed on Scopus.

Table 2-4: Most Cited Papers (global citations)

	Paper	*DOI*	*TC*	*TC per Year*
1	BALDUZZI M, 2014, ACM INT CONF PROC SER	10.1145/2664243.2664257	111	11.10
2	CHANG CH, 2021, RELIAB ENG SYST SAF	10.1016/j.ress.2020.107324	87	29.00
3	HOSSAIN NUI, 2019, RELIAB ENG SYST SAF	10.1016/j.ress.2019.04.037	78	15.60
4	DE LA PEÑA ZARZUELO I, 2020, J IND INFOR INTEGR	10.1016/j.jii.2020.100173	61	15.25
5	POLATIDIS N, 2018, COMPUT STAND INTERFACES	10.1016/j.csi.2017.09.006	57	9.50
6	TAM K, 2019, WMU J MARIT AFF	10.1007/s13437-019-00162-2	49	9.80
7	CARRERAS GUZMAN NH, 2020, SYST ENG	10.1002/sys.21509	46	11.50
8	BOLBOT V, 2020, SAF SCI	10.1016/j.ssci.2020.104908	40	10.00
9	SVILICIC B, 2019, J NAVIG	10.1017/S0373463318001157	37	7.40
10	CAPROLU M, 2020, IEEE COMMUN MAG	10.1109/MCOM.001.1900632	29	7.25

The first observation is that there is much **computer** security-related literature. For example, Balduzzi et al. (2014) present a security evaluation of AIS (Automatic Identification System), by introducing threats affecting both the implementation in online providers and the protocol specification.

Then, there is literature related to **risk management** (and parts of the process such as risk identification, analysis and assessment). Hossain et al. (2019) develop a Bayesian network for assessing and quantifying the resilience of a deep-water service port. Tam and Jones (2019) present a framework for maritime cyber-risk assessment, whereas Svilicic et al. (2019b) present a risk analysis to identify and categorise cyber threats to ships. Bolbot et al. (2020) present an interesting cyber-risk assessment method and as a case study they apply their method for the cyber-risk assessment, and design enhancement of the navigation and propulsion systems of an inland waterways **autonomous vessel.** A clear connection between cyber security and autonomous shipping has been actually identified by the literature review. In addition. Chang et al. (2021) presents a novel methodology for evaluating risk related to hazards associated with autonomous shipping using a Failure Modes and Effects Analysis (FMEA) method in conjunction with Evidential Reasoning (ER) and Rule-based Bayesian Network (RBN) to quantify the risk levels of the identified hazards. It identifies 'cyber-attacks' as the second most important hazard.

Most Frequent Words and Trend Topics

In order to identify trending topics and areas into which research is focusing, the most frequent words that appear in the list of keywords are presented in Table 2-5 and Figure 2-13, abstracts and titles of the selected papers. As expected, words such as cyber-security (and all related spellings) and the other keywords used in our search do appear at the top of the list.

Table 2-5: Most frequent words in keywords, abstracts and titles (occurrences)

	AUTHORS' KEYWORDS		*ABSTRACTS*		*TITLE*	
	Words	**#**	**Words**	**#**	**Words**	**#**
1	cybersecurity	35	maritime	590	maritime	101
2	cyber security	22	cyber	440	cyber	77
3	maritime	21	security	341	security	58
4	maritime cyber security	18	systems	323	cybersecurity	54
5	risk assessment	14	system	206	systems	30
6	maritime cybersecurity	11	cybersecurity	189	risk	23
7	maritime security	11	risk	170	ship	20
8	ais	9	information	155	system	18
9	cyber-security	9	paper	151	assessment	15
10	security	8	ships	132	industry	15
11	navigation safety	7	data	127	analysis	14
12	risk management	7	industry	123	framework	14
13	cyber risk	6	threats	122	autonomous	13

There are some interesting observations that can be made. For example, the words/keywords risk, risk assessment and risk management appear very frequently, same with the keywords ‘AIS’ and 'navigation safety'. This highlights the fact that most of the published research has focused on the management of cyber threats and applications related to IT systems (such as the AIS) and navigational safety. This is something that has already been identified and discussed in the previous section.

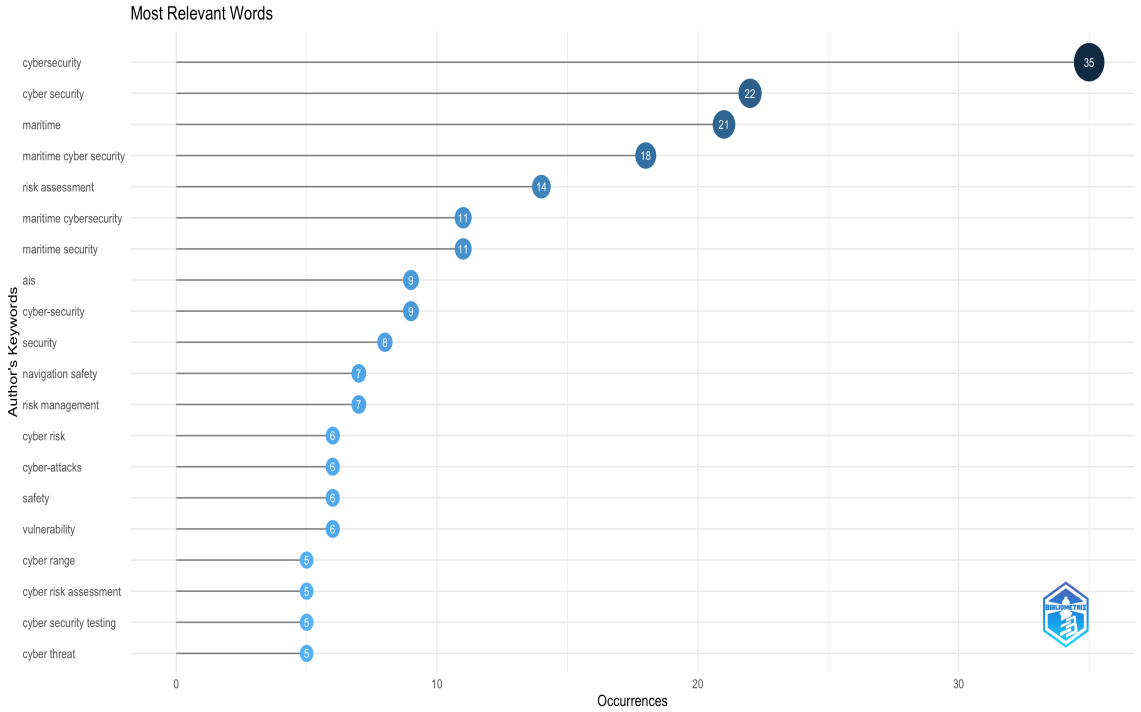


Figure 2-13: Most Frequent Keywords - Source: Author's analysis using Bibliometrix

Co-word Analysis and Thematic Maps

Co-word analysis draws clusters of keywords which can be considered themes. Properties such as density and centrality can be used in classifying them and mapping them in a two-dimensional diagram; see Figures 2-14 and 2-15.

Figure 2-14 depicts the co-word network, representing the cognitive structure of the network based on the co-occurrence of words in the abstract, title, or keywords within the paper. The most frequently used words include "cyber security," "cybersecurity," "ship," and "network security." These words exhibit strong connections among themselves, indicating that research in maritime cybersecurity is closely linked to advancements in network security.

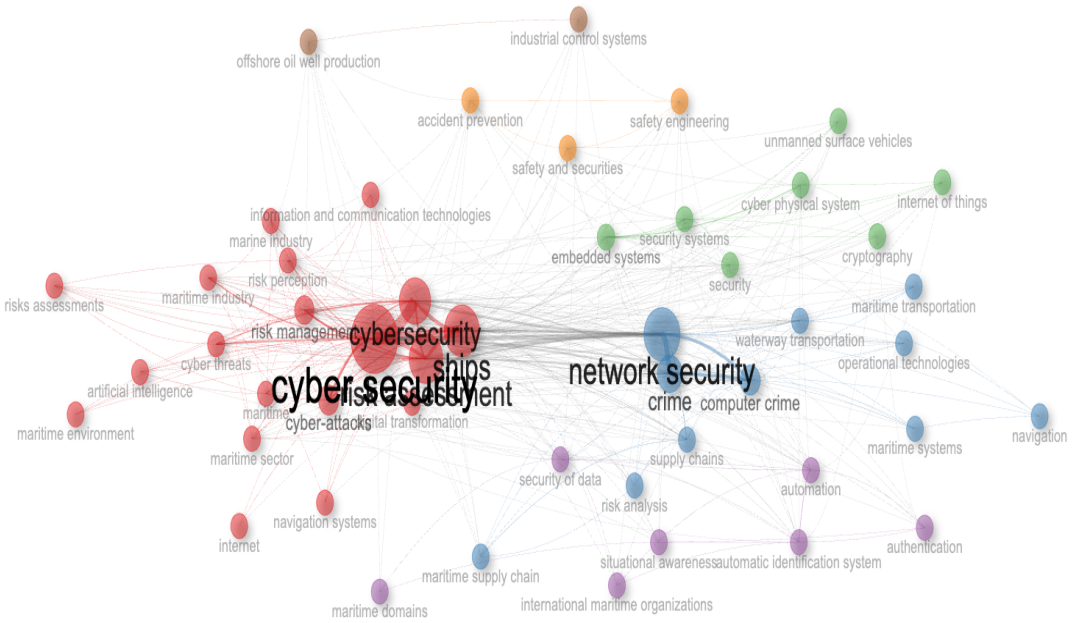


Figure 2-14: Co-word Network - Source: Author's analysis using Bibliometrix

The thematic map (see Figure 2-15) presents themes according to the quadrant in which they are placed: (1) upper-right quadrant: motor themes; (2) lower-right quadrant: basic themes; (3) lower-left quadrant: emerging or disappearing themes; (4) upper-left quadrant: very specialised/niche themes. Motor themes present strong centrality and high density and therefore are the key research themes; emerging or disappearing themes are themes that are relatively weak, and then the basic themes are relevant but not well-developed ones. This analysis can help us identify existing themes and potential areas for future research (such as related to port attacks, IMO regulations, analysis of critical infrastructure and other topics as presented in the upper-right quadrant). Again, it is obvious that risk-based approaches are key in addressing the relevant threats.

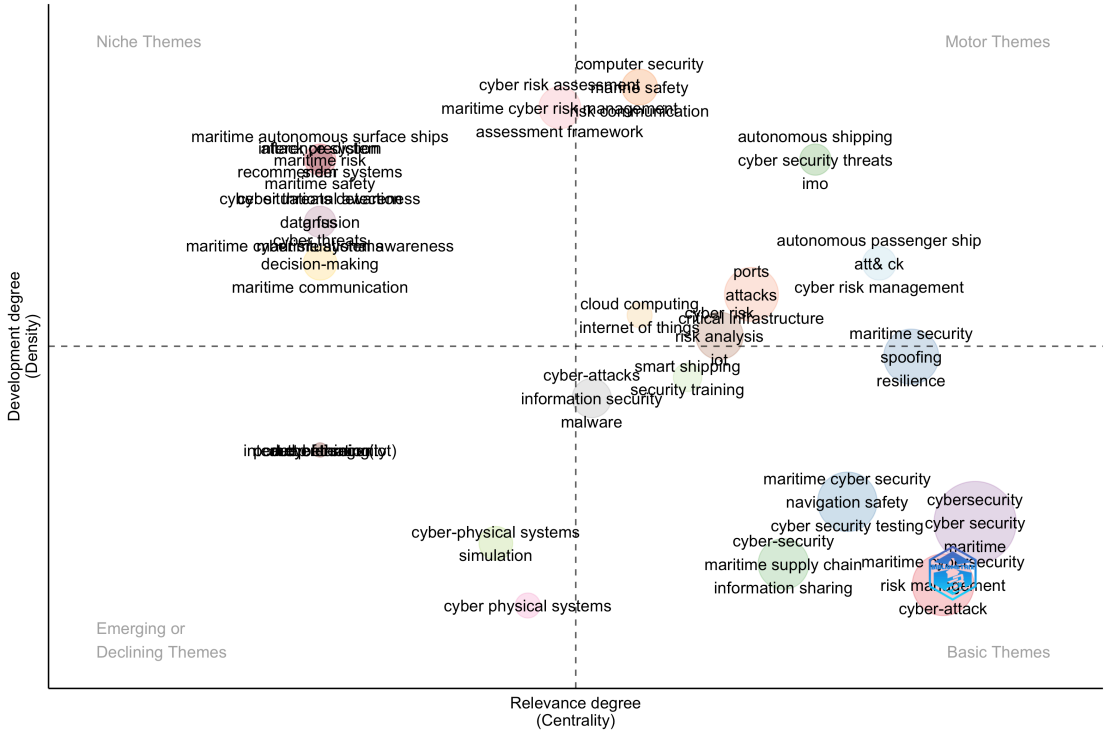


Figure 2-15: Thematic Map by uthors' keywords - Source: Author's analysis using Bibliometrix

2.11.3 Review of the Academic Literature

Based on the above results and the discussion in the Introduction (Ch. 1), this thesis will address the topic using a risk-based approach, which is the dominant approach in the literature.

Below, the key references are presented, which are also summarised in Table 2-6.

In the academic literature, a number of cybersecurity risk assessment and management in the maritime industry based either on the technologies could be found, some of them are generic, and others are specific to the maritime domain.

Kalogeraki et al. (2018a) proposed a knowledge management methodology and an associated measurement which can share supply chain knowledge and suggests ways for identifying cyber threats over critical infrastructure and maritime logistics and supply chain (MLoSC). It includes identifying cyber threats, mitigating methodology and evaluating mitigate methodology. As a result, the three more vulnerable onboard Cyber Physical Systems (CPSs) were identified, and appropriate cybersecurity controls were identified.

Kalogeraki et al. (2018b) analysed recent risk management policies that have significant limitations for regarding the security requirements for ICTs, Internet of Things (IoT) platforms, satellites, and time installations, which are crucial to maritime logistics and supply chain (MLoSC) services. Therefore, they proposed a novel risk assessment methodology designed to consider the particularities and specificities of SCADA infrastructures and CPSs in the maritime logistics industry. They figured outed most MLoSC stakeholders believe that supply chain participants must have security controls.

Hareide et al. (2018) analysed the enhancement of navigation systems by cybersecurity. They addressed that cyberattacks can pose a number of attack vectors to vessels, as well as the plausibility and consequences of such attacks. Furthermore, in order to enhance navigators' competence, they provide a practical example of how one can demystify cyber threats.

Hossain et al. (2019) researched different identified factors for port resilience using a Bayesian network and different advanced techniques such as forward propagation, backward propagation, sensitivity analysis, and information theory. According to the formal interpretation of these analyses, maintenance, alternative routing, and manpower restoration improve a port infrastructure system's resilience in disruptive environments.

Svilicic et al. (2019a) proposed maritime cyber risk assessment through computational vulnerability scanning of the Electronic Chart Display and Information System (ECDIS) on Kobe University’s training ship and conducting a survey for ship crew. They determined cyber threats on the vessel and detected cyber vulnerabilities of ECDIS. They insisted this assessment process offers guidelines for minimizing cyber risks on ships and enhancing the cyber security level of ship cyber critical systems.

Svilicic et al. (2019b) addressed the cyber security resilience examination of an onboard integrated navigational system (INS) applied on a RoPax vessel engaged in global trade. They identified threats analysed qualitatively to determine in order to determine how

cyber risks threaten the INS. As a result, vulnerabilities in the INS operating system indicate a need for occasional maintenance in addition to regulatory compliance.

Tam and Jones (2019) proposed the Maritime Cyber-Risk Assessment (MaCRA) framework model to present maritime cyber risk and provide information for cybersecurity decision-makers in the maritime sector. They provided several demonstration scenarios about plausibility and intentional cyberattacks in the past, and then they informed vulnerabilities of maritime systems. They insist that the MaCRA framework will provide accurate and quantifiable cyber risk assessments so that the maritime community can identify the most significant cyber risks and profitably mitigate them by employing security solutions and continuously improving cybersecurity across the global fleet.

Guzman et.al (2020) examine the key features of Cyber Physical Systems (CPSs) and their relationship with other system types; define the dependencies between levels of automation vessel and human roles in CPSs from a system engineering perspective; and apply systems thinking to describe a multi-layered diagrammatic representation of CPSs for combined safety and security risk analysis, demonstrating an application in the maritime sector to analyse an autonomous surface vessel.

Kavallieratos and Katsikas (2020) addressed the STRIDE and DREAD methodologies to qualitatively and quantitatively assess the CPSs for digitalised vessels in the maritime industry. STRIDE is an acronym for 'Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege', which are six security threats. DREAD is an acronym for 'Damage, Reproducibility, Exploitability, Affected users/systems, and Discoverability'. They identified appropriate baseline cyber security controls for each of the three more vulnerable onboard CPSs.

Bolbot et al. (2020) proposed an enhanced novel method for cybersecurity risk assessment of ship systems with the Cyber-Preliminary Hazard Analysis method, which is used to assess cyber-risks and enhance navigation and propulsion systems of

autonomous inland waterways vessels. According to the result of research, attacking the shore control centre could have the highest potential for terrorists, and Malware could infect the collision avoidance system and the situation awareness system. Another finding is that the safety of the investigated vessel system can be improved by adding firewalls on the conduits between control zones, developing redundancy and implementing intrusion detection.

Yoo and Park (2021) identified cybersecurity risk factors in the maritime industry that are managed by the ship safety management system (SMS), and through the itemised risk assessment, vulnerabilities can be prioritised for improvement. They identify cyber risk components based on the best practices proposed by IMO guidelines, BIMCO guidelines, ISO/IEC 27001 international standards and figure out the three areas of administrative, technical, and physical security. Through Analytic Hierarchy Process (AHP) analysis, the top three priorities for mitigating maritime cybersecurity risks are as follows:

"Increasing awareness of risks and educating staff about mitigation measures; Controlling access to cyber networks; Improving threat detection and blocking systems".

Enoch et al. (2021) introduced an assessment method for evaluating the security of onboard ship network systems and presented a novel framework called the Maritime Vessel-Hierarchical Attack Representation Model (MV-HARM). This model is designed to identify vulnerabilities and threats in vessel network systems, assess vessel networks with single or multiple cyberattack goals, analyse vessel architectures for attack scenarios, and compare the effectiveness of defence mechanisms across various vessel attack cases.

Gunes et al. (2021) addressed applying an integrated cybersecurity risk assessment method for container ports by analysing four cyberattack scenarios which are applied an integrated cybersecurity management approach based on container terminal cyber-physical assets. They found that critical infrastructures face a new threat today from cyberattacks, especially in ports utilising cyber-physical systems heavily.

Kechagias et al. (2022) approached to present maritime cybersecurity aspects from an inside view and proposed a detailed case study analysis of cybersecurity in the maritime sector. They addressed ISO 90001 quality management system PDCA approach (Plan-Do-Check-Act cycle). Through conducting a survey, they identified there is no list of remote access to the ship, and lack of cybersecurity practice have been executed for the ship.

Numerous studies have explored maritime cybersecurity, concentrating on specific situations within the sector. However, there is a noticeable gap in investigations related to identifying cyber threats and implementing risk control measures in this context. The remaining part of this thesis aims to fill this void by providing an overview of general maritime cybersecurity threats and proposing comprehensive risk control measures. By broadening the scope beyond specific scenarios, this research seeks to contribute valuable insights into the overall landscape of maritime cybersecurity risk assessment, aiding in the development of robust strategies to safeguard maritime cyber systems and infrastructure from potential cyber threats.

Table 2-6: Summary of the key academic maritime cyber risk-related literature

Authors /Year	Ship/Port	Summary	Methodology
Kalogeraki et al.(2018a)	Maritime supply chain	Identifying cyber threats, mitigate methodology and evaluating mitigate methodology.	Knowledge management
Kalogeraki et al.(2018b)	Maritime supply chain	Proposed a novel risk assessment methodology designed to take into account the particularities and specificities of SCADA infrastructures and CPSs.	Novel Integrated Risk Management System
Hareide et al. (2018)	Ship	Provide a practical example of how one can demystify cyber threats.	Situational Awareness, Cyber kill chain model
Hossain et al. (2019)	Port	Maintenance, alternative routing, and manpower restoration improve a port infrastructure system's resilience.	BN
Svilicic (2019a)	Ship	Evaluate the cybersecurity level of the ECDIS system on the vessel.	Risk matrix
Svilicic (2019b)	Ship	Cyber security resilience examination of a shipboard INS installed on a RoPax ship engaged in international trade.	mixed-method approach, combining an interview and cyber security testing of the INS
Tam and Jones (2019)	Ship	Developed Maritime Cyber Risk Assessment (MaCRA) Framework.	MaCRA framework
Guzman et al. (2020)	Ship	Examines the key features of CPSs, defines the dependencies.	A real scale test that incorporates autopilot mode and a collision avoidance system (COLAV).
Kavallieratos and Katsikas (2020)	Ship	Identified baseline cyber security controls for each of the three more vulnerable on-board CPSs.	STRIDE and DREAD methodologies
Bolbot et al. (2020)	Ship	Propose an enhanced novel method for cybersecurity risk assessment of ship systems.	Cyber-Preliminary Hazard Analysis
Yoo and Park (2021)	Ship	Identified and rank cybersecurity risk factors in the maritime industry.	AHP, risk matrix
Enoch et al. (2021)	Ship	Proposed a novel framework and security risk modelling.	MV-HARM
Gunes et al. (2021)	Port	Through analysing four classical cyberattack scenarios, they propose to apply an integrated cyber risk assessment method for a container port with a cyber-physical perspective.	Integrated cyber security risk management modelling
Kechagias et al. (2022)	Ship	Presenting a shipping company's cybersecurity systemic approach with references to policies and procedures with research practice	Risk assessment matrix.

2.12 Conclusions

In Chapter 2, a number of definitions of risk and risk-related vocabularies are provided, including risk, threat, vulnerability and cyber risk management (RCM) from IMO Guidelines (MSC-Fal.1/Circ.3), BIMCO Guidelines version 4, US NIST Cybersecurity Framework version 1.1 and BS EN ISO/IEC 27000:2020 Information security management. This helps to distinguish the differences among these terms.

Several safety-related risk management frameworks are also reviewed. For example, ISO 31000:2018 and IEC 31010:2019, with more definitions of the risk management process, risk assessment, risk analysis, risk evaluation, and risk treatment. IMO Formal Safety Assessment (FSA) with five steps. In addition, this research reviews cybersecurity-related risk management frameworks; some of them are generic, and others are specific to the maritime domain. For example, IMO Guidelines (MSC-Fal.1/Circ.3 and MSC-Fal.1/Circ.3/Rev.1) suggest that effective cyber risk management in the maritime sector should follow the following five function elements, including 'Identify', 'Protect', 'Detect', 'Respond' and 'Recover'. This is the same as NIST Cybersecurity Framework. BIMCO-led Guidelines on Cyber Security Onboard Ships suggests the following six steps as a cycle for the cyber risks management approach, including 'Identify threats', 'Identify vulnerabilities', 'Assess risk exposure', 'Develop protection and detection measures', 'Establish response plans' and 'Respond to and recover from cyber security incidents'.

Two IMO codes are reviewed for maritime cybersecurity management, e.g., International Ship and Port Facility Security Code (ISPS) and International Safety Management (ISM) code. Several classifications societies-led publications for maritime cybersecurity are also reviewed, including Det Norske Verutas (DNV) 'Cyber security resilience management for ships and mobile offshore units in operation' (DNVGL-RP-G496), which mentions the applications of bowtie analysis in the maritime cybersecurity management. Lloyds Register (LR) LR Cyber Security Framework (CSF) for the Marine and Offshore sector, based on IMO Resolution MSC.428(98) and IMO Guidance MSC-FAL.1/Circ.3. American Bureau of Shipping (ABS) 'Guide for Cybersecurity Implementation for the Marine and Offshore Industries' that highlight mitigation

measures applied to IT and OT systems for maritime assets. Korean Register (KR) also published marine cybersecurity guidelines in 2019 to strengthen safety against internal and external cyber threats for IT technologies and services introduced and operated by onboards and offshores.

The previous sections have presented various risk definitions and key approaches to managing risk for safety and cyber security applications. Furthermore, bibliometric analysis and the relevant literature, including both academic papers and sources in the grey literature, have been presented. In fact, there are few excellent literature survey papers already published; therefore, a detailed analysis of the relevant literature was not presented. There are referred to Progoulakis et al. (2021) and Bolbot et al. (2022) for two very comprehensive surveys of the maritime cybersecurity domain; the latter also summarises the relevant literature survey papers. Progoulakis et al. (2021) present the relevant standards, guidelines and a survey of relevant academic papers, with risk analysis and assessment methods being the main focus of their survey. Bolbot et al. (2022) present a bibliometric analysis and a very comprehensive review of the area, along with the research directions. In line with our findings and the work of Progoulakis et al. (2021), their analysis demonstrated that the main research focus in maritime cybersecurity is indeed on *"the development or application of cybersecurity risk assessment techniques and the design of monitoring and intrusion detection tools for cyberattacks in maritime systems".*

Current research often lacks a well-established method for quantifying and assessing the risks associated with maritime cybersecurity. Additionally, there is a notable absence of tools or methods to link high-risk cybersecurity threats with appropriate countermeasures, and a lack of visualisation solutions to facilitate this connection, especially within the maritime industry. Consequently, the field of research focused on cybersecurity in the maritime industry is still in its early stages. Most existing studies primarily concentrate on improving general cybersecurity measures, while investigations specifically addressing individual cyber threats and strategies to reduce associated risks are rare. This gap extends to the scarcity of scholarly endeavours aimed

at conceiving a comprehensive framework for the evaluation of cybersecurity risks pertinent to maritime operations.

Based on the above, more existing literature on this topical area needs to be explored. The expansion of the body of literature on autonomous shipping leads us to anticipate that cybersecurity will increasingly attract research attention. As the level of autonomy will be increasing, so will the dependence of ships on IT and OT systems, increasing the overall cybersecurity risks; see, for example, Chang et al. (2021), who have identified 'cyberattacks' as the second most important hazard for autonomous vessels.

3

METHODOLOGY OF THE THESIS

3.1 Introduction

As we have seen in the previous chapters, shipping is a key enabler of international trade which is indeed a very old industry. There have always been risks, piracy for example is not a new risk but in the past decades the number of incidents has definitely been increased. Nowadays, security issues have a new meaning as the introduction of digitalisation has brought cybersecurity risks at the forefront.

Cyberattacks they do not need to be sophisticated. Even a simple action, like a seafarer opening an email attachment on their personal computer connected to the ship's network, can lead to serious problems. Failures to address these attacks could result in severe consequences, including human fatalities, asset and reputation loss, economic damages, and environmental repercussions. Both the literature review (presented in Chapter 2) and the industry approaches, especially at the IMO level, are focused on addressing cybersecurity using risk management approaches. As we have seen in Sections 2.3 and 2.4., the IMO in particular has a long tradition of using risk-based approaches; see for example the Formal Safety Assessment, Goal-based Standards, and the recent discussion on risk-based assessment tools to address risks for autonomous vessels, also referred to as Maritime Autonomous Surface Ships (MASS).

Thus. it comes to no surprise that the IMO has introduced a risk-based approach to deal with cybersecurity; see Section 2.4.2 for a discussion on the BIMCO-led Guidelines on Cyber Security Onboard Ships). We have also seen a growing focus on risk management in academic literature and especially in its subprocesses such as risk identification, risk analysis and risk assessment). What might come to surprise thought, is that the current approaches are not systematic, are too general and, thus, ineffective.

Based on this gap, as identified and largely discussed in Section 2, our overall methodology relies on a risk-based approach and more specifically follows the widely used risk assessment concept. In line with the risk assessment steps, such as identification, analysis, and evaluation, this research contains the identification, analysis, and evaluate cyber threats and risk control measures. Despite having a robust approach, there is also a need for rigorous data collection and a comprehensive analysis to arrive at meaningful results. To that extend, this chapter presents the research design, data collection, procedure, data analysis, and, finally, a validity and reliability analysis.

3.2 Research Design

In this chapter, the research design of this thesis is introduced. As observed in Chapter 1, contemporary research frequently lacks a firmly established methodology for quantifying and evaluating risks inherent in maritime cybersecurity. Furthermore, a noticeable gap exists in terms of tools or methodologies that can effectively correlate high-risk cybersecurity threats with suitable countermeasures. More visualisation solutions need to be designed to facilitate this connection, particularly within the maritime industry. Therefore, this thesis seeks to establish a comprehensive framework for the management of cybersecurity risks in the maritime industry, intended to serve as a fundamental reference for future research initiatives.

Now, the risk step in assessing risks is to identify them. We obtain a list of potential hazards/threats through the literature and using a suitable methodology we rank them (see Section 3.4 below). Ranking them is important as we need to focus our attention

on the threats that are associated with high risks. This is of paramount importance given also the rather limited resources that companies have to address cybersecurity threats.

Thus, at the beginning, the research will rank cybersecurity threats and assess risk control measures in the maritime sector. This will be accomplished by analysing the literature review and utilising data obtained from a survey of maritime experts. The approach involves integrating existing academic research findings and expert opinions. In conclusion, the intention is to visually present the maritime cybersecurity risk assessment procedure through a case study.

During the primary data analysis in Chapters 4 and 5, the framework of this thesis is systematically employed, encompassing risk management steps such as risk identification, analysis, and evaluation (refer to Figure 1-1). In each chapter, specific methodologies are applied. Chapter 4 utilises Failure Modes and Effects Analysis (FMEA) and a Rule-based Bayesian Network (RBN) to rank maritime cybersecurity threats (the 1st and 2nd steps of the risk management steps in Figure 1-1). Meanwhile, Chapter 5 employs the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) to identify the effectiveness of risk control measures (the 3rd and 4th steps in Figure 1-1). Further details regarding the application of each method will be presented in the subsequent sections and elaborated upon in their respective chapters. This approach ensures a thorough exploration of risk management processes and provides a clear understanding of the methods employed for analysing and evaluating maritime cybersecurity risks.

To accomplish this, questionnaire surveys were carried out in Chapters 4 and 5 to gather empirical data based on the experiences and opinions of maritime experts. This research not only introduces a framework for maritime cybersecurity but also performs risk assessments and evaluates risk control measures using first-hand empirical data obtained from industry experts, avoiding sole reliance on secondary data. The experts are sea crew, academia, and people who work in shipping companies; the responder's detail is described in Chapter 4; incorporating subjective data through expert judgment

ensures that the results truly reflect stakeholders' experiences and best practices. This approach provides practical insights, offering a real-world perspective on the current state of maritime cybersecurity. The proposed framework and empirical approach guarantee their relevance and applicability in addressing present challenges within the maritime cybersecurity landscape. Thus, the research not only outlines a framework for maritime cybersecurity but also systematically assesses risks and appraises risk control measures based on empirical insights derived directly from industry experts, enhancing the robustness and practicality of the findings.

3.3 Data Collection and Sampling

In this research, three questionnaire surveys were distributed through Google Forms and email. Questionnaires 1 and 2 are to categorise and rank cybersecurity threats, and Questionnaire 3 is to identify the effectiveness of risk control measures. In order to collect more replies from various regions, each questionnaire is designed with three versions: English, Korean and Chinese. Additionally, due to the COVID-19 pandemic during the research period, conducting face-to-face interviews for data collection was challenging. Furthermore, considering the saving of the research period, cost, and convenience of respondents, an online survey was a more efficient option than phone calls, video calls, or printed paper surveys.

The selection of participants, particularly for expert opinions, is crucial for obtaining reliable data. The questionnaires in this thesis utilised non-probability sampling, specifically purposeful sampling, which relies on judgment to select participants based on their expertise and accessibility. To maximise responses, experts were also asked to recommend others, creating a snowball effect—a method consistently applied across all questionnaires in this thesis, employing a technique known as 'snowball sampling.'

3.4 Procedures

In Chapter 4, a systematic literature review is first conducted to identify a list of maritime cyber threats, which is the first step of risk assessment in Figure 2-2. In order to analyse the threats (this is the next step), we first evaluate the threats in a more general way (Questionnaire 1) to select the more important ones by ranking their mean values. After identifying the relative important threats, we apply a more advanced method to analyse the selected threats in detail. Based on the threats selected in Questionnaire 1, we analyse the most threat rankings from marine industry experts who have extensive experience in the marine industry and are familiar with the subject of cybersecurity opinions (Questionnaire 2) using FMEA-RBN. After that, a sensitivity analysis is conducted to validate the analysis model.

In Chapter 5, risk control measures are identified via a literature review and six criteria, leading to the identification of seven risk control options. To evaluate the effectiveness of risk control options, we conduct an online questionnaire survey (Questionnaire 3). We analyse the importance criteria of cybersecurity and evaluate the ranking of risk control measures, obtaining respondents' opinions using Fuzzy TOPSIS. This involved the use of seven linguistic terms, ranging from "very poor" to "very good."

The logical flow of the research is illustrated in Figures 3-1, and the process and result of the chapters are presented in detail in each chapter.

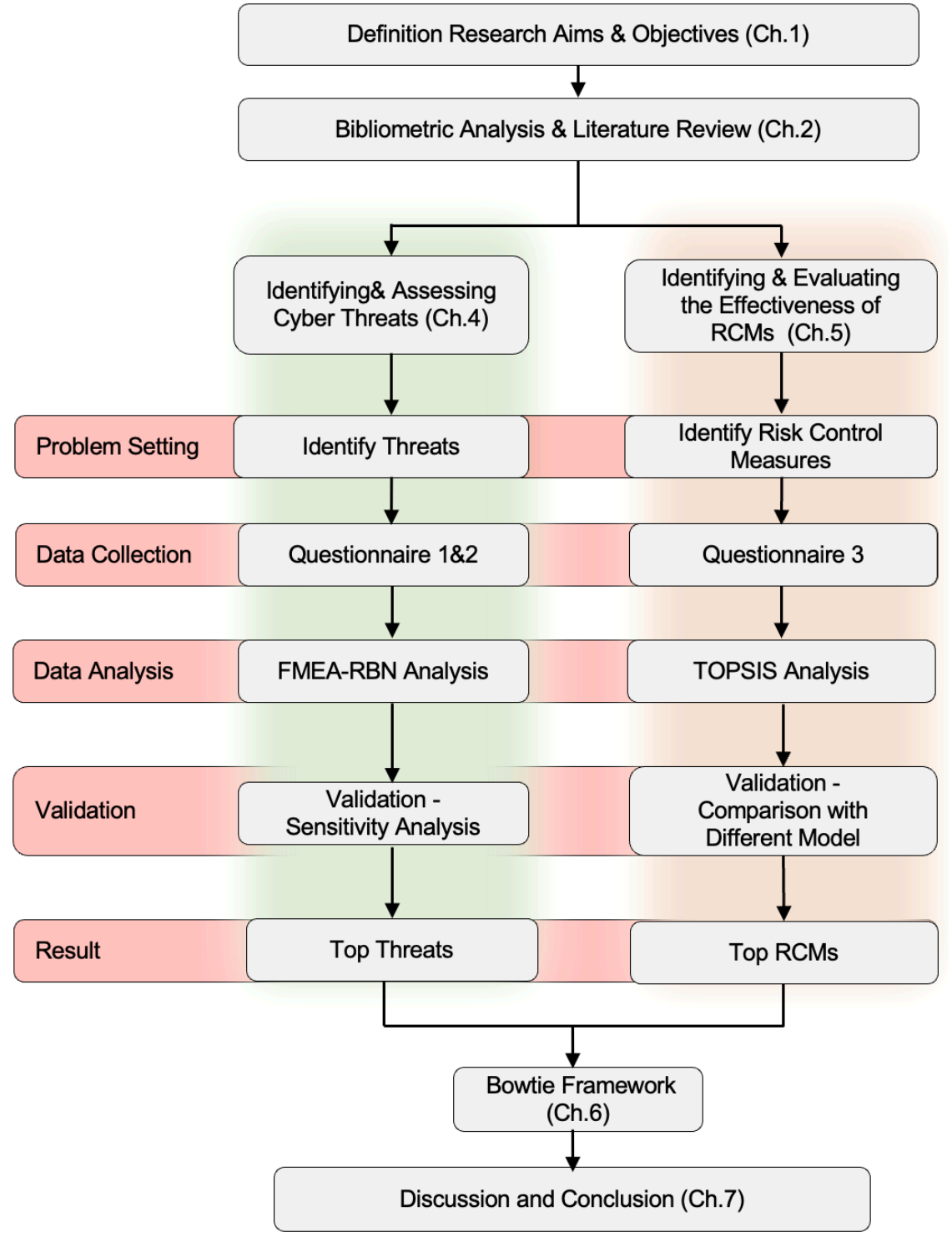


Figure 3-1 The logical flow of the research

3.5 Data Analysis

3.5.1 Risk Assessment Methods

A risk assessment involves evaluating potential incidents' likelihood, consequences, and tolerances (Aven, 2016; Evrin, 2021). It is an integral component of a comprehensive risk management strategy steps (identification, assessment, response and monitoring) to implement control measures to mitigate or eliminate potential risk-related consequences. The primary objective of conducting a risk assessment is to prevent adverse outcomes associated with risks and, concurrently, to assess potential opportunities that may arise. In essence, risk assessment serves as a proactive and preventive measure, guiding the identification and management of risks to enhance overall decision-making and safeguard against potential negative impacts (Ostrom and Wilhelmsen, 2019).

3.5.2 Qualitative Method

The qualitative risk analysis in cybersecurity aims to identify specific risks requiring detailed scrutiny and determine appropriate controls and actions based on their potential impact on objectives (Yoo and Park, 2021). This approach is broadly applicable to all cybersecurity risks, aiding in the swift identification of areas related to routine cybersecurity functions. For instance, it can assess whether undetected risk concerns are linked to identified cybersecurity risk areas. Subsequently, the quantitative risk analysis in cybersecurity delves into specific risk scenarios, providing detailed information for more informed decision-making. By combining qualitative and quantitative methodologies, organisations can gain a comprehensive understanding of cybersecurity risks, enabling the implementation of effective measures to address and manage potential cybersecurity challenges (Evrin, 2021).

3.5.3 Quantitative Method

Quantitative risk analysis is a method applied to high-priority and/or high-impact cybersecurity risks (Apostolakis, 2004). This approach assigns numerical or quantitative ratings to these risks, facilitating a probabilistic assessment of business-related issues within the cybersecurity domain. However, its widespread application in all

cybersecurity projects or processes, particularly those managed with a project management approach, is limited (Evrin, 2021). The extent of its use depends on factors such as the specific cybersecurity project, associated risks, and the availability of data for quantitative analysis. In cybersecurity, quantitative risk analysis, and realistic and measurable data are used to calculate impact values based on the probability of occurrence. This methodology relies on mathematical and statistical foundations, allowing for the expression of risk values in monetary terms (Eckhart et al., 2019). This capability extends the usefulness of the results beyond the assessment context, providing organisations with a tangible understanding of the potential financial implications of identified cybersecurity risks. While not universally applicable, quantitative risk analysis in cybersecurity offers a detailed and measurable perspective, particularly valuable for high-priority cybersecurity risks, aiding organisations in making informed decisions regarding risk mitigation strategies (Sheehan et al., 2021).

The qualitative method is rapid yet subjective, while the quantitative method, although meticulous and objective, demands more time and complexity in collecting data (Evrin, 2021). Although time is one of the main limitations of using the quantitative method, this can be overcome by strict timetable planning. This research thus opted for quantitative analysis over qualitative analysis, relying on objective data derived from experts' opinions and experience to identify current maritime security issues.

3.5.4 FMEA-RBN

Chapter 4 endeavours to gauge and evaluate the risk levels associated with maritime cybersecurity threats by employing a blend of Failure Modes and Effects Analysis (FMEA) and a Rule-based Bayesian Network (RBN). The initial phase of the risk analysis involves identifying noteworthy cyber threats prevalent in the maritime sector. A comprehensive literature review has revealed six dimensions for categorising maritime cyber threats. These dimensions provide a structured framework for the subsequent risk assessment, enabling a systematic analysis of potential vulnerabilities and their corresponding impacts on maritime cybersecurity.

Evrin (2021) addressed that there are several tools and techniques that can be used in quantitative risk analysis. Those tools and techniques are shown below:

- ***"Heuristic methods:*** *Techniques based on experience or expertise for estimating contingency.*
- ***Three-point estimate:*** *A method utilizing optimistic, most likely, and pessimistic values to derive the best estimate.*
- ***Decision tree analysis:*** *A graphical representation illustrating the consequences of selecting various alternatives.*
- ***Expected monetary value (EMV):*** *A methodology for establishing contingency reserves in project or business process budgets and schedules.*
- ***Monte Carlo analysis:*** *A technique employing optimistic, most likely, and pessimistic estimates to determine business costs and project completion dates.*
- ***Fault tree analysis (FTA) and failure modes and effects analysis (FMEA):*** *The examination of a structured diagram that identifies elements contributing to system failure".*

This research employs a hybrid methodology that combines Failure Modes and Effects Analysis (FMEA) with a Rule-based Bayesian Network (RBN) to conduct a comprehensive examination of the risk levels associated with identified categories and threats in maritime cybersecurity, utilising the GeNIe software. Recognizing the underreporting of cyber threats, the FMEA concept is applied with three parameters—the likelihood of failure, consequence of failure, and probability of undetected failure—as the initial step in maritime cyber risk assessment (Alyami et al., 2019; Chang et al., 2021; Park et al., 2023). Conventional risk assessment approaches face challenges in handling high-uncertainty risk data in maritime cybersecurity, necessitating the use of more advanced techniques. The proposed FMEA-RBN methodology provides several advantages in maritime cybersecurity, particularly its capability to integrate both objective and subjective data. This integration is crucial in situations where historical data is limited or unreliable due to a restricted number of incidents. By incorporating subjective data from

expert judgment, the methodology ensures that the results encompass stakeholders' experiences and best practices.

3.5.5 Fuzzy TOPSIS

Chapter 5 is dedicated to the identification and evaluation of cybersecurity Risk Control Measures (RCMs). Effectively addressing relevant risks is pivotal for mitigating the consequences of cyberattacks. The process involves the identification of threats and vulnerabilities, as well as the formulation of protective and detection measures to diminish these risks. The overarching goal is to minimize the likelihood of vulnerabilities being exploited and/or the severity of their impact. To offer high-level recommendations, RCMs are expressed in broad terms.

The most commonly utilised RCMs, referred to as 'alternatives' in Multiple Criteria Decision-Making terminology, were identified through a literature review. In this research, the Fuzzy theory is employed in conjunction with the Technique for Order of Preference by Similarity to the Ideal Solution (TOPSIS) method due to its visibility and ease compared to other Multiple Criteria Decision-Making (MCDM) techniques. The assessment and ranking of the most widely used RCMs are conducted against six criteria identified through a comprehensive state-of-the-art literature review and analysed using an R-package.

MCDM methods have been employed for various purposes, such as selecting a preferred alternative, categorizing alternatives, and ranking alternatives based on subjective preferences (Behzadian et al., 2012). Numerous methods fall under the MCDM umbrella, with the most prevalent ones being TOPSIS, Analytic Hierarchy Process (AHP), Best-Worst Method (BWM), Grey Relational Analysis (GRA), among others. Table 3-1 delineates the characteristics of these MCDMs.

Table 3-1: The characteristics of MCDM

Methods	Characteristic
TOPSIS	TOPSIS compares distances between alternatives to ideal and negative ideal solutions to evaluate alternative options based on multiple criteria. It provides a systematic approach for decision-makers to rank and select the best alternatives. (Behzadian et al., 2012; Bakioglu and Atahan, 2021).
AHP	AHP is an approach to decision-making that structures complex decisions into a hierarchy, involves pairwise comparisons of criteria and alternatives, uses mathematical calculations to derive priorities, and synthesises judgments to provide a systematic method of ranking and selecting alternatives (Vaidya and Kumar, 2006; Rahman et al., 2021).
BWM	BWM is a decision-making technique that focuses on identifying the best and worst alternatives based on pairwise comparisons of their relative importance. It is characterised by its simplicity, relative importance scores, and focus on extremes rather than comprehensive ranking (Rezaei, 2016; Gupta and Baruna, 2017).
GRA	Grey Relational Analysis is a method for comparing and analysing data sequences with uncertain or incomplete information. It is characterised by its use of grey numbers, relative comparison, and its applicability in decision-making and predictive analysis in cases where traditional statistical methods may not be suitable (Manikandan et al., 2017; Hasanzadeh et al., 2023).

Based on the nature of this research, AHP and TOPSIS are the most suitable methods to rank the importance of the RCMs. Table 3-2 illustrates a summary of the advantages and disadvantages of AHP and TOPSIS per Oguztimur (2011), Karthikeyan et al. (2016), Alsalem et al. (2018), Wang (2018), Canco et al. (2021).

The choice of employing TOPSIS in this study stems from the difficulties encountered in acquiring valid data from respondents and the inherent limitations of AHP. AHP traditionally requires respondents to provide data for relative comparisons. Consequently, TOPSIS was deemed more suitable for this particular task, circumventing the challenges associated with data collection in AHP. The decision to opt for TOPSIS is

driven by its compatibility with the research's unique circumstances and the need to ensure a feasible and accurate assessment process, given the complexities associated with the chosen criteria and alternatives.

Table 3-2: Pros and Cons of TOPSIS and AHP

	Pros	Cons
TOPSIS	**Ease of Use**: TOPSIS is user-friendly and suitable for decision-makers with various backgrounds (Alsalem et al.,2018). **Complex Decision Support**: It is effective for complex decisions with multiple criteria, particularly when managing conflicting objectives (Wang, 2018). **Comprehensive Analysis**: TOPSIS considers multiple criteria, offering a holistic view of the decision problem (Alsalem et al.,2018; Wang, 2018). **Clear Rankings**: It provides clear and visual rankings of alternatives, aiding decision-makers in understanding option performance (Alsalem et al.,2018; Wang, 2018).	**Linear Assumption**: TOPSIS assumes linear relationships between criteria and alternatives. It may not yield accurate results when non-linear relationships are present. (Alsalem et al.,2018). **Ties in Rankings**: When two or more alternatives have the same closeness values in the TOPSIS ranking, determining their exact order of preference can be challenging (Wang, 2018).
AHP	**Structured Approach**: AHP provides a structured framework for decision-making, improving clarity and comprehension (Oguztimur, 2011; Karthikeyan et al., 2016). **Flexibility**: It is adaptable to a wide range of decision scenarios, making it versatile (Oguztimur, 2011; Karthikeyan et al., 2016; Alsalem et al.,2018). **Quantitative and Qualitative Integration**: It can handle both quantitative and qualitative data, allowing diverse information types to be incorporated into the decision-making process (Oguztimur, 2011; Wang, 2018; Canco et al., 2021).	**Complexity**: AHP can be complex, especially in large decision problems with many criteria and alternatives, the process of conducting pairwise comparisons and calculations can become complex and time-consuming. (Karthikeyan et al., 2016; Canco et al., 2021). **Subjectivity**: AHP relies on subjective judgments from decision-makers, which can introduce bias and variation into the results (Alsalem et al.,2018; Canco et al., 2021). **Elicitation Challenges**: Obtaining accurate and consistent judgments from decision-makers, particularly when dealing with numerous criteria, can be difficult (Canco et al., 2021).

3.6 Validity and Reliability of Analysis

Due to the different research methods applied in the technical chapters, the validity and reliability analyses of each chapter are described as follows:

In Chapter 4, sensitivity analysis has been extensively employed in the validation of the proposed Bayesian Network (BN) model. Various approaches can be utilised for this purpose. For instance, Yang et al. (2008) conducted sensitivity analysis by adjusting the percentage of a linguistic level using Excel, while Yu et al. (2020) and Chang et al. (2021) focused on changes in specific linguistic levels using the GeNIe software. In this study, sensitivity analysis is conducted to assess the impact of identified cyber threats on overall risk through GeNIe. The results of the sensitivity analysis are expected to adhere to two Axioms: 1) An increase/decrease in the probabilities of each cyber threat should generate a relative increase/decrease to the risk. 2) Given the variation of the probability distributions of each cyber threat, its influence magnitude on the risk values should keep consistency (refer to 4.3.2 step 6), indicating the robustness of the proposed model. The detailed results of the sensitivity analysis are presented in section 4.3.4 of Chapter 4.

In Chapter 5, in order to validate the results of the fuzzy TOPSIS approach, we actually compare our results with those of similar or alternative approaches that could have been used. In fact, conducting sensitivity analysis is crucial to assess the influence of slight variations in inputs on the final ranking, such as the impact of different weights. However, performing sensitivity analysis in a fuzzy environment poses challenges, particularly when dealing with fuzzy weights rather than precise numerical values. To validate both the findings and the appropriateness of the selected method, we applied the same input data to established Multiple Criteria Decision-Making (MCDM) methods, including Fuzzy VIKOR, Fuzzy WASPAS, and Fuzzy Multi-Objective Optimization by Ratio Analysis (MOORA). A comprehensive discussion of these methods is beyond the scope of this research (refer to Ceballos, 2017, for a comparative analysis). Nevertheless, as indicated in Table 4-10, all the methods yielded comparable rankings for our input data.

This noteworthy result underscores the robustness of our findings. In practical terms, this implies that employing alternative methods would likely yield similar results, affirming the validity of our managerial and policy implications. Possible limitations of this approach are discussed in conclusion part (see Section5.5) but based on the fact that all these different methods arrive at similar results (i.e. ranks) there is strong evidence that the results are robust.

3.7 Summary of Chapter

This chapter employs the methodology to grasp the research aim and structure. The methodology revolves around risk assessment steps, with each technical chapter employing the FMEA-RBN and Fuzzy TOPSIS methods for assessment and evaluation. The applied methodologies are introduced in this chapter, accompanied by a review justifying their use. The specific processes and results are expounded upon in the relevant sections of each chapter.

4

AN ASSESSMENT OF MARITIME CYBERSECURITY RISKS

4.1 Introduction

Cybersecurity risks are becoming a growing concern within the maritime industry, particularly with the rapid advancement of digital technologies, including autonomous shipping. There is substantial evidence, as indicated in Chapter 1 Table 1-1 and 1-2, that cyberattacks targeting the maritime sector have been on the rise over time. This escalation in cyber-attacks has prompted an increased focus on maritime cybersecurity research in the past 3-4 years. The maritime industry plays a pivotal role in the global economy, and any disruptions to maritime operations can profoundly impact the global supply chain (UNCTAD, 2022). Cyberattacks have the potential to disrupt maritime operations in several ways, such as disabling critical systems, compromising sensitive data, or causing financial losses. Consequently, the shipping industry has grown increasingly concerned about cybersecurity in recent years due to factors such as the expanded use of IT systems, automation, and digitisation. These technologies are employed onboard vessels for tasks such as navigation, engine and power management, and damage control systems monitoring, giving rise to significant concerns regarding maritime cybersecurity.

Risk assessment has been traditionally used to manage safety; in the aftermath of the 9/11 attacks shipping has become a target of what Lu et al. (2022) refer to as 'non-traditional safety events', which include piracy attacks and terrorism. However, the increasing reliance on IT leads to new challenges e.g., the introduction of cyber-related risks in shipboard operations (Karim, 2020). Digitalisation is also one of the main priorities of some ports (see for example Campisi et al., 2022) as they are using automation and innovative technologies to improve their performance. There is thus, now, the need to shift the focus from traditional safety and security towards cyber risks. Cyber risks need to be addressed in a proactive and systematic way hence the need for risk assessment. The importance of cybersecurity in the maritime industry is widely acknowledged, but there is a paucity of research on the specific cybersecurity threats and risk control measures that are relevant to this sector. This is a significant gap in knowledge, as it hinders the development of effective cybersecurity strategies for the maritime industry. In order to facilitate research on maritime cybersecurity, this chapter aims to fill the current research gap by identifying maritime cyber threats, evaluating their risk levels and proposing countermeasures to improve maritime cybersecurity.

Several traditional risk assessment methods have been utilised in the maritime sector, such as Hazard and Operability Studies (HAZOP), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), and Failure Mode and Effects Analysis (FMEA) (Wan et al., 2019a; Fan et al., 2020). Although there is a growing number of maritime cybersecurity studies, and international organisations have already published maritime cybersecurity guidelines, research addressing maritime cybersecurity risk assessment remains limited. It often leans towards practical industry-driven perspectives and lags behind compared to other industries, such as aviation (Suciu et al., 2019), autonomous vehicles (Khan et al., 2022), and healthcare (Coventry and Branley, 2018).

Current maritime cybersecurity risk assessment is typically conducted using either qualitative analysis or very traditional quantitative risk analysis methods, such as bowtie analysis (Progoulakis et al., 2021) and risk matrices (Yoo and Park, 2021). However, security risks in general, and cybersecurity risks in particular, are prone to high data

uncertainty. This sometimes raises questions about the utility of traditional risk approaches and the reliability of the risk estimation results. Hence, there exists a significant research gap regarding the incorporation of advanced uncertainty modelling to enhance maritime cybersecurity risk quantification and estimation, as elaborated in detail in Section 2.1.

This chapter aims to use the combination of FMEA and Rule-based Bayesian Network (RBN) to estimate and prioritise the risk levels of maritime cybersecurity threats. FMEA and RBN have several advantages in dealing with high uncertainty in risk data and, therefore, have attracted increasing interest within risk assessment involving high uncertainty in data in recent years and used in various maritime-related research related to, for example, maritime supply chains (Wan et al., 2019a), autonomous ships (Chang et al., 2021), and container shipping services (Zhou et al., 2022). Its advance in tackling risk data fits well with maritime cybersecurity risk assessment given the very limited historical data available due to the limited number of accidents that occurred in the past. It is because of the high uncertainty in cybersecurity-related risk data that there are few studies on maritime cybersecurity risk analysis and fewer related to the use of advanced quantitative models for quantitative risk analysis of maritime cybersecurity. To the best of my knowledge, this is the first attempt to use a combined FMEA and RBN approach to address maritime cybersecurity risks. This research will therefore make new contributions, a theoretical one which is presenting a novel cybersecurity risk analysis methodology based on FMEA-RBN and a practical one, the ranking of cybersecurity threats in maritime operations.

4.2 Identification of Maritime Cyber Threats

As discussed above due to the importance of the topic, companies must address and manage the related cybersecurity risks. Measures to control the risks should be sought with urgency. Before doing so though, the relevant threats need to be identified and consequently efforts should be focused on the most important ones; the latter could be achieved by prioritising the threats.

As the first step of risk analysis, one should start with the identification of significant cyber threats in the maritime domain. Indeed, many cyberattack accidents have been reported involving common cyber threats such as phishing, malware, ransomware, DDoS (Distributed Denial of Service), and man in the middle attack (Ren et al., 2017; Corallo et al., 2022). Through a literature review, six dimensions to categorise the maritime cyber threats are identified, including ‘Phishing’, 'Malware’, ‘Man in the middle attack’, ‘Thief of credentials’, ‘Human factor’, and ‘Using outdated IT systems’; see Table 4-1 for the threats discussed in the relevant literature. The detailed information of the threats is provided in the following sections.

Table 4-1: List of reviewed papers and articles

	Phishing	Malware	Man in the middle attack	Theft of credentials	Human factor	Using outdated IT systems
Sen (2016)		√				√
Jones et al (2016)		√				√
DNV (2016)		√			√	√
IHS Markit (2016)	√	√		√		
IMO (2017a)		√				
Boyes and Isbell (2017)		√		√	√	
BIMCO (2018)	√	√			√	√
IHS Markit (2018)	√	√	√	√		
Tam and Jones (2018)	√	√			√	√
Park et al. (2019)	√	√			√	
Mraković and Vojinović (2019)	√	√	√	√		
Svilicic et al (2019b)		√	√			
Alcaide and Llave (2020)	√	√			√	
Androjna et al. (2020)		√			√	
Bolbot et al. (2020)	√	√	√		√	√
Karahalios (2020)		√			√	
Meland et al. (2021)	√	√				
Senarak (2021)	√	√		√	√	√
Farah et al. (2022)	√	√	√			√
Khan et al. (2022)		√			√	
Tusher et al. (2022)	√			√	√	√
Vu et al. (2023)	√	√	√		√	
Karaca and Söner (2023)	√	√			√	

4.2.1 Phishing

Phishing refers to sending a seeming impersonation email with links to fake websites, downloading malicious files (Qbeitah and Aldwairi, 2018) or text (Yeboah-Boateng and Amanor, 2014). The email may show that it is from a bank or other various valid businesses. Once the user clicks the links, all the information the user inputs to the fake website will be transferred to the hacker. These emails can be very deceiving and even an experienced user can be cheated. Sea crews using personal devices (e.g., smartphone, tablet, private USB device) could cause cybersecurity issues by receiving phishing emails or visiting malicious websites, and thus installing malicious viruses into vessel operational systems (BIMCO, 2018; Meland et al., 2021; Farah et al., 2022).

4.2.2 Malware

Malware is malicious software that assesses or damages devices without the knowledge of the user, and further spreads the virus by downloading files attached to infected emails or accessing a fake website or connecting USB drives and removable media containing malicious malware (Pham et al., 2010). It could lead to ransomware attacks or even Distribute Denial of Service (DDoS) (Jones et al., 2016; Farah et al., 2022). In the maritime sector, IMO (2017a) and BIMCO et al. (2018) have also listed malware as a severe threat to maritime cybersecurity given that malware could access and damage the operation systems of vessels or steal sensitive data from shipping companies. Meland et al. (2021) have listed a number of maritime cyberattacks caused by malware between 2010 and 2020. According to Mraković and Vojinović (2019), malware constitutes a major type of cyberattack in the maritime industry. Additionally, Alcaide and Llave (2020) argue that malware is the primary choice of threat for carrying out malicious activities aimed at breaching maritime cybersecurity.

4.2.3 Man in the middle attack

Through man in the middle attacks, hackers can intercept all communication between different parties and/or impersonate these parties. Hackers conceal their presence in free/open Wi-Fi hotspots or fake websites, preventing users from sending and receiving data or even redirecting the information to another user (Mallik, 2019; Suciu et al., 2019;

Vu et al., 2023). In the maritime industry, this cyber threat commonly targets remote desktop protocol (RDP) services running on the Electronic Chart Display and Information System (ECDIS) (Svilicic et al., 2019a).

4.2.4 Theft of credentials

Theft of credentials is a type of cyber threat that involves stealing proof of identity from users or customers. Insecure login systems and simple passwords are easily targeted by hackers (Imran and Nizami, 2011). Boyes and Isbell (2017) suggested that certain threat actor groups may breach servers or websites to pilfer users' credentials. A survey conducted by IHS Markit and BIMCO revealed that out of 300 stakeholders in the maritime sector, 65 respondents reported experiencing cyber threats, with 25% of them indicating that they had encountered credential theft attacks (IHS Markit, 2016). According to the 2018 IHS Markit survey, instances of credential theft increased significantly, rising from 2% in 2017 to 28% in 2018 (IHS Markit, 2018).

4.2.5 Human factors

For shipping safety and security incidents, the human factor has been recognised as a critical element that directly and indirectly contributes to around 80-90% of accidents (Heij and Knapp, 2018; Chang et al., 2021). From a cybersecurity perspective, stakeholders lacking knowledge of cybersecurity systems and failing to adhere to cybersecurity processes render systems vulnerable to cyber accidents (Boyce et al., 2011). Erstad et al. (2022) tackled the issue of the lack of seafarers' cybersecurity awareness through a case study. Presently, seafarers use vessel computer and control systems without due caution. Despite certain computers being designated for specific purposes, such as ECDIS workstations, seafarers tend to utilize them for other activities like watching TV or playing solitaire. Seafarers do not perceive this as a problem, given that cyber threats are not adequately addressed. On the other hand, insider threats, wherein individuals within the organisation may act for personal gain or specific purposes, such as stealing vital data, also exist (Mazzarolo and Jurcut, 2019). Human factors are indeed considered a primary threat to maritime cybersecurity (Park et al., 2019; Senarak, 2021; Tusher et al., 2022; Karaca and Söner, 2023). Hopcraft and Martin

(2018) argued that the advancement of maritime industry technology has introduced more opportunities for the industry to be exposed to cyber threats due to unintentional human errors.

4.2.6 Using outdated IT systems

Sen (2016), Jones et al. (2016), and BIMCO (2018) analysed the vulnerability of maritime cybersecurity and found that shipping companies were excessively reliant on outdated technology and were using outdated versions of antivirus software, which posed major threats. For instance, some staff still believe that antivirus software and firewalls can fully protect systems from cyberattacks. Without an up-to-date IT system, hackers can target vessels or companies through viruses or malware, which are challenging to detect and defend against using traditional antivirus software (Sen, 2016; Park et al., 2019; Farah et al., 2022; Tusher et al., 2022). Additionally, many current ships were constructed long before the industry began considering cybersecurity as a significant concern. Consequently, some ships and shipping companies continue to use outdated IT and OT systems that are susceptible to cyberattacks.

Upon analysis of the identified cyber threats, it is apparent that viral infection does not stand alone as a singular threat. Cybersecurity risks can emanate from various sources, including the misbehaviour or errors of seafarers and the inexperienced management of devices by the company. To effectively mitigate these cybersecurity threats, a comprehensive approach is imperative, encompassing considerations from human, technical, and policy perspectives.

4.3 Methodology

A hybrid method of FMEA with an RBN is employed to investigate the risk levels of the identified maritime cyber categories and threats in detail. Several traditional risk assessment methods have been utilised in the maritime sector such as the use of Delphi and risk matrices (Chang et al., 2015; Wan et al., 2019b), Hazard and Operability Studies (HAZOP), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), FMEA (Wan et al., 2019a;

Fan et al., 2020); more recent approaches focus also on risk-based resilience (Wan et al., 2022). Considering not all cyber threats are detected and reported, this chapter applies the concept of FMEA with three parameters (i.e., likelihood of failure, consequence of failure and probability of the failure being undetected) as the initial step of maritime cyber risk assessment. However, traditional risk assessment methods are not able to deal with the high uncertainty risk data in maritime cybersecurity; a more advanced technique should therefore be employed. The newly proposed FMEA-RBN methodology has revealed several advantages within the context of maritime cybersecurity.

A key advantage of the model is its ability to incorporate both objective and subjective data; this is important when historical data is often unavailable or not reliable given the small number of the occurred accidents. The use of subjective data obtained through expert judgement also ensures that the results reflect the stakeholders experience and best practices. The inference process involving BN can inherently overcome one of the weaknesses of traditional FMEA which is the assumption that all three FMEA-parameters contribute equally towards the risk factor of an event (Hassan et al., 2022). In addition, the methodology can account for the difference in the experience and expertise of the experts; this could be done by setting different weights. RBN has been selected to build up the risk model in this paper due to its advantages such as modelling uncertain and complex domains (Uusitalo, 2007; Khan et al., 2021; Chen et al., 2022).

Although there are a few attempts on using RBN in the maritime industry, ostensibly this is the first attempt to use a combined FMEA and RBN approach to address maritime cybersecurity risks. The main novelties in terms of risk modelling are:

a) new definitions and descriptions of the three cybersecurity risk parameters and the linguistic terms used to define each of them and

b) new conditional probability distribution to model the conditional relationship between the risk parameters and cybersecurity levels.

In addition, with the validation through a sensitivity analysis, RBN provides a more reliable model and results. The details of FMEA and RBN are discussed in the following sections.

4.3.1 Failure Modes and Effects Analysis (FMEA)

FMEA is a common method for investigating the importance of potential failure modes and is widely used for safety and reliability analysis in products and processes (Yang et al., 2008; Wan et al., 2019a). FMEA refers to risk in terms of severity, likelihood of failure mode/cause and detection; as per the IEC 60812:2018 standard. It should be noted here that FMEA has been employed to address cybersecurity threats. For instance, Asllani et al. (2018) proposed a 'cybersecurity FMEA (C-FMEA) process' and reviewed the relevant literature. Haseeb et al. (2021) analysed cybersecurity in an Internet of Things environment, while Kennedy et al. (2021) addressed human factors and cybersecurity in the context of the Australian rail industry using FMEA. For consistency, the traditional FMEA terminology is retained, and from this point onward, any reference to 'failures' or 'failure modes' denotes threats.

Risk Priority Number (RPN), denoted by S, is the main component of FMEA and derived by combining assessments made on ordinal scales with values for the likelihood of maritime cyberthreat (L), their consequences (C) and probability of them being undetected (P) as follows:

$$\boldsymbol{S = L \times C \times P}$$

When lacking historical failure data, the three parameters are often defined by linguistic terms in order to better describe and model subjective assessments (Yang et al., 2008; Alyami et al., 2019). The Likelihood of threats (L) is determined using five linguistic terms (Li, i=1,2, …, 5): very low, low, average, high, and very high. Consequence (C) is estimated by five terms (Ci, i=1,2, …, 5): negligible, marginal, moderate, critical, and catastrophic. The Probability of the failure being undetected (P) is determined using the following five terms (Pi, i=1,2, …, 5): highly unlikely, unlikely, average, likely, and highly likely. The

definitions of the five levels for these three parameters are shown in Tables 4-2, 4-3, and 4-4. Finally, the RPN for each threat is defined using five linguistic terms (Si, i=1,2,…, 5): very low, low, average, high, and very high.

Table 4-2: The definition of likelihood for maritime cybersecurity
- Source: adapted from Alyami et al. (2019) and Chang et al. (2021)

Likelihood of maritime cyberthreat	Definition
Very Low (VL)	The cyberthreat is rare but might happen during lifetime
Low (L)	The likelihood of the threat is around once a year
Average (A)	The likelihood of the threat is occasional (e.g., once a quarter)
High (H)	The likelihood of the threat is repeated (e.g., once a month)
Very High (H)	The likelihood of the threat is almost certain

Table 4-3: Definition of consequences for maritime cybersecurity
- Source: adapted from Alyami et al. (2019) and Chang et al. (2021)

Consequence of maritime cyberthreat	Definition
Negligible (N)	The consequence of the threat is limited. It only requires a minor maintenance
Marginal (MA)	The threat causes a marginal system damage. The system operations are slightly interrupted. It requires a short period (e.g., less than 6 hours) to fix the system.
Moderate (MO)	The threat causes a moderate system damage. The system operations are interrupted. It requires a longer period (e.g., more than 12 hours) to fix the system.
Critical (CR)	The threat causes a major system damage. The system operations need to be stopped. High degree of operational interruption occurs
Catastrophic (CA)	The threat causes a total system loss. Extremely serious consequence that affects sailing operations occurs.

Table 4-4: Definition of the probability of the threat being undetected for maritime cybersecurity - Source: adapted from Alyami et al. (2019) and Chang et al. (2021)

Probability of the failure being undetected	Definition
Highly unlikely (HU)	The threat could be detected without checks or maintenance
Unlikely (U)	The threat could be detected by regular checks or maintenance
Average (A)	The threat could be detected by intensive checks or maintenance
Likely (L)	The threat is difficult to be detected by intensive checks or maintenance
Highly likely (HL)	The threat is impossible to be detected even by intensive checks or maintenance

4.3.2 FMEA Rule-based Bayesian Networks (FMEA-RBN)

It is adapted the approach proposed by Yang et al. (2008) and apply it within the new maritime cybersecurity context by defying the following six steps:

(1) Identify the threats in maritime cybersecurity

(2) Develop the Bayesian network

(3) Establish rule-based systems with degree of belief (DoB) in FMEA-RBN

(4) Aggregate rules with a Bayesian Reasoning mechanism

(5) Convert the results into crisp values with utility functions

(6) Validate using sensitivity analysis

Step 1: Identify threats in maritime cybersecurity

Based on the literature review and the results of Questionnaire 1, six maritime cyber threat categories are identified, including 'Phishing', 'Malware', 'Man in the middle attack', 'Theft of credential', 'Human factor', and 'Using outdated IT systems'. Each threat category consists of several threats.

Step 2: Develop the Bayesian network

After the identification, the threat categories and threats are further used to build up a BN model. Figure 4-1 illustrates the developed BN model to be used in this study; threats

are illustrated with yellow ovals (root nodes) and threat categories are represented with orange ovals (leaf nodes).

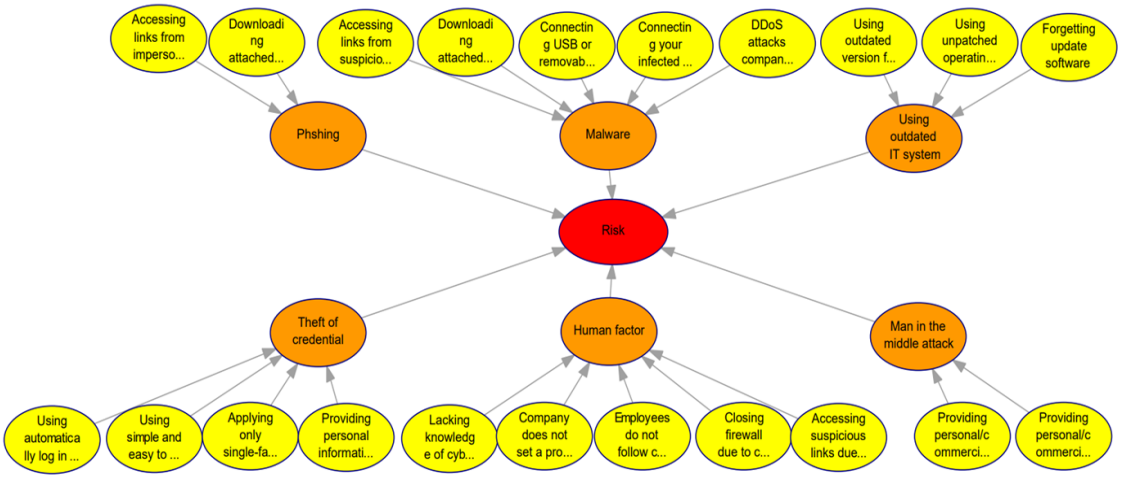


Figure 4-1: The maritime cybersecurity Bayesian network model - Source: Author

Step 3: Establish rule-based systems with a DoB in FMEA-RBN

A rule-based approach is applied to define the causation relationships and impact levels among the nodes of the BN. It uses several rules to describe the relationship between the *IF* and *THEN* parts, which are used to convert p attendance attributes {A1, A2, …, Ap} (IF part) into q states {C1, C2, …, Cq} (THEN part) by assigning a belief degree β_s (s=1, 2, …, q) to Cs $(s \in q)$. For example, the w^{th} IF-THEN rule (denoted as R_w) in a rule-based set can be expressed as:

$$R_w: \textbf{IF } A_{w1} \text{ and } A_{w2} \text{ and } \ldots \text{ and } A_{wp}, \textbf{ THEN } \{(\beta_{w1}, C_1), (\beta_{w2}, C_2), \ldots, (\beta_{wq}, C_q)\}.$$

The *IF* part is a set of linguistic states $A^w=\{A^w_1, A^w_2, \ldots, A^w_p\}$ in a R_w , and a set of DoB in the *THEN* part can be expressed as $\{(\beta^w_1, C_1), (\beta^w_2, C_2), \ldots, (\beta^w_q, C_q)\}$for the description of how each C_s $(s=1, 2, \ldots, q)$ is the believed to be the result of β_s, which can be assigned with experience or by using converting methods (e.g., equivalent influential method from Yang, et al. (2008). After combining all rules of R, it can then develop a rule-based structure with multiple-input and multiple-output.

When conducting the IF-THEN rules, this research applies a belief structure that helps us to identify the respondents' knowledge of the specific threats. The rules with belief

structures in FMEA can be established based on expert judgments. Table 4-5 shows a three-parameters DoB distribution with the 125 rules (5^3).

Table 4-5: The established RBN with a belief structure

Rule	**Parameters in the IF part**			**DoB in the THEN part**				
No	**L**	**C**	**P**	**S1**	**S2**	**S3**	**S4**	**S5**
1	Very low (L1)	Negligible (C1)	Very unlikely (P1)	1				
2	Very low (L1)	Negligible (C1)	Unlikely (P2)	0.67	0.33			
3	Very low (L1)	Negligible (C1)	Average (P3)	0.67		0.33		
4	Very low (L1)	Negligible (C1)	Likely (P4)	0.67			0.33	
5	Very low (L1)	Negligible (C1)	Very likely (P5)	0.67				0.33
…	…	…	…	…	…	…	…	…
121	Very high (L5)	Catastrophic (C5)	Very unlikely (P1)	0.33				0.67
122	Very high (L5)	Catastrophic (C5)	Unlikely (P2)		0.33			0.67
123	Very high (L5)	Catastrophic (C5)	Average (P3)			0.33		0.67
124	Very high (L5)	Catastrophic (C5)	Likely (P4)				0.33	0.67
125	Very high (L5)	Catastrophic (C5)	Very likely (P5)					1

As per the above-mentioned approach, several rules are used in the FMEA-RBN maritime cybersecurity model. For example, an *IF-THEN* rule to describe the relationship among the three parameters in the FMEA-RBN is defined as follows:

R1: IF very low (L1), negligible (C1), and very unlikely (P1),

THEN the S is {(1, very low risk (S1)), (0, low risk (S2)), (0, average (S3)), (0, high risk (S4)), (0, very high risk (S5))}.

R2: IF very low (L1), negligible (C1), and unlikely (P2),

THEN the S is {(0.67, very low (S1)), (0.33, low (S2)), (0, average (S3)), (0, high (S4)), (0, very high (S5))}.

They can further be explained as:

R1: if likelihood of the threat is very low, consequence is negligible, and probability of the failure being undetected is very unlikely, then the risk level of the threat is very low with a 100% DoB, low with a 0% DoB, average with a 0% DoB, high with a 0% DoB, and very high with a 0% DoB.

R2: if likelihood of the threat is very low, consequence is negligible, and probability of the failure being undetected is unlikely, then the risk level of the threat is very low with a 67% DoB, low with a 33% DoB, average with a 0% DoB, high with a 0% DoB, and very high with a 0% DoB.

Step 4: Aggregate rules through a Bayesian Reasoning mechanism

The observation information (e.g., obtained through expert judgement) are aggregated by using the Bayesian Reasoning mechanism, in which a BN is developed for information aggregation. In the BN, a graphical network, firstly, describes the relationships of root nodes to the leaf node. A conditional probability table (CPT) for each node is, then, developed by converting the *IF-THEN* rules (i.e., DoB in the THEN part of each rule) into a CPT. Table 4-6 presents the CPT for the risks used in the FMEA-RBN methodology.

Table 4-6: The conditional probability table (CPT) for the FMEA-RBN

L	**L1**								**L5**							
C	**C1**				**C5**				**C1**				**C5**			
P	**P1**		**P5**		**P1**		**P5**		**P1**		**P5**		**P1**		**P5**	
S1	1		0.67		0.67		0.33	…	0.67		0.33		0.33		0	
S2	0	…	0	…	0	…	0		0	…	0	…	0	…	0	
S3	0		0		0		0		0		0		0		0	
S4	0		0		0		0		0		0		0		0	
S5	0		0.33		0.33		0.67		0.33		0.67		0.67		1	

In Table 4-6, the first rule of the threat level (yellow level in Figure 4-1) can be expressed as follows: R_1: IF L1, C1 and P1, THEN {(1, (S1)), (0, (S2)), (0, (S3)), (0, (S4)), (0, (S5))}. Where represent a condition that if L1 and C1 and P1, the probability of S(DoB) is p (R|L1, C1, P1) = (1, 0, 0, 0, 0).

For the category level (orange level in Figure 3-1), there are different numbers of threats under each category. For example, 'Phishing' and 'Man in the middle attack' have 2 threats (5^2=25 rules), 'Using outdated IT system has 3 threats (5^3=125 rules), theft of credential has 4 threats (5^4= 625 rules), and 'Human factor' and 'Malware' have 5 threats (5^5=3125 rules). To save space, it is presented the 5th rule of phishing as follows:
R5: IF Phishing threat 1 is very high, and Phishing threat 2 is very low, THEN the risk of 'Phishing' is {(0.5, (S1)), (0, (S2)), (0, (S3)), (0, (S4)), (0.5, (S5))}.

In terms of the overall risk (red level in Figure 3-1) that has 6 threat categories (5^6=15625 rules), and the 195th rule for overall risk can be expressed as follows:
R_{195}: IF 'Phishing' is very high, 'Malware' is very high, 'Man in the middle attack' is high, 'Theft of credential' is average, 'Human factor' is low, and 'Using outdated IT systems' is very low, THEN the overall risk is {(0.33, (S1)), (0.17, (S2)), (0.17, (S3)), (0.17, (S4)), (0.17, (S5))}.

From the above illustrative examples, it can be seen that the DoB assigned in the THEN parts are based on the proportion distribution with the condition of each element in the IF part carrying the same weight.

Once the model is developed, the prior probabilities, which is the observed information, will be aggregated to calculate the marginal probabilities. After analysing the prior probabilities of all nodes, the marginal probability p(Rh) for the result can be calculated as follows (Yang et al., 2008):

$$p(R_h) = \sum_{i=1}^{5}\sum_{j=1}^{5}\sum_{k=1}^{5} p\left(R\middle|L_i, C_j, P_k\right)p(L_i)p\left(C_j\right)p(P_k)\,, (h = 1, \dots, 4)$$

Step 5: Convert the results into crisp values with utility functions

A set of utility values are assigned to the nodes in the FMEA-RBN model to illustrate the importance of threats from different scenarios. In this chapter, they are combined to prioritise the threats and threat categories. For example, from low-risk influence on high-risk influence, the utility values assigned to L, C and Pare UL1=UC1=UP1=1; UL2=UC2=UP2=2, UL3=UC3=UP3=3, UL4=UC4=UP4=4 and UL5=UC5=UP5=5 (Chang et al., 2021). On this basis, five IF-THEN rules (see Table 3-6) are used to combine the utility values for R, including Rule 1, Rule 32, Rule 63, Rule 94 and Rule 125, in which

R1: IF L1, C1 and P1, THEN {(1, (R1)), (0, (R2)), (0, (R3)), (0, (R4)), (0, (R5))};

R32: IF L2, C2 and P2, THEN {(0, (R1)), (1, (R2)), (0, (R3)), (0, (R4)), (0, (R5))};

R63: IF L3, C3 and P3, THEN {(0, (R1)), (0, (R2)), (1, (R3)), (0, (R4)), (0, (R5))};

R94: IF L4, C4 and P4, THEN {(0, (R1)), (0, (R2)), (0, (R3)), (1, (R4)), (0, (R5))};

R125: IF L5, C5 and P5, THEN {(0, (R1)), (0, (R2)), (0, (R3)), (0, (R4)), (1, (R5))}.

Therefore,

$$U_{R1} = U_{L1} * U_{C1} * U_{P1} = 1$$

$$U_{R2} = U_{L2} * U_{C2} * U_{P2} = 8$$

$$U_{R3} = U_{L3} * U_{C3} * U_{P3} = 27$$

$$U_{R4} = U_{L4} * U_{C4} * U_{P4} = 64$$

$$U_{R5} = U_{L5} * U_{C5} * U_{P5} = 125$$

The crisp values (CV) are calculated by using the utility function below:

$$CV = \sum_{z=1}^{t} p(R_h)\, U_z$$

where t is the number of linguistic terms of a node, $p(R_h)$ the marginal probability and U_{Rz} (z = 1, 2, 3, 4, 5) the synthesised utility value assigned to R. Utility values can be then assigned to calculate the risk levels of all the threats and threat categories and express

them into crisp values for a risk ranking purpose. The larger the value, the higher the associated security risk is.

Note that in this work a linear utility function is used in line with the literature, see for example Wan et al. (2019a), Yu et al. (2020) and Chang et al. (2021). At the same time, it is assumed equal importance for threats and threat categories. Weights could have been used to assign, for example, greater importance to the opinion of, say, specific experts or specific threats/categories. This would have required more evidence though as to why specific experts or different threats are more important than others, a more complex questionnaire and potentially a more complex methodology e.g., the use of Evidential Reasoning (Yu et al., 2020).

Step 6: Model validation

Sensitivity analysis refers to the sensitivity of the model's performance to changes in parameters (Ren et al., 2008). It can help determine the model's reliability. Sensitivity analysis is widely used in BN analysis and can be conducted in different ways. For example, Yang et al. (2008) conducted sensitivity analysis by adjusting the percentage of a linguistic level using Excel, while Yu et al. (2020) and Chang et al. (2021) focused on changes in several specific linguistic levels using the GeNIe software. In this study, a sensitivity analysis is conducted to analyse how the identified cyber threats affect the overall risk through GeNIe. Additionally, an added step of validation is performed. If the model is robust, it should satisfy at least the following two axioms (Jones et al., 2010):

Axiom 1. An increase/decrease in the probabilities of each cyber threat should generate a relative increase/decrease to the risk.

Axiom 2. Given the variation of the probability distributions of each cyber threat, its influence magnitude on the risk values should keep consistency.

4.4 Data Analysis

4.4.1 Result of the First Run Questionnaire

To analyse the risk level of the six identified maritime cyber threat categories and a list of threats, a methodology is developed. The threats and the categories identified from the literature are first validated and initially evaluated by domain maritime experts to make sure that they are comprehensive and representative. A semi-structured questionnaire with a five-point Likert scale (Questionnaire 1; Appendix A) is distributed to experts who work in relevant stakeholders such as shipping companies, port operators and academia. The structure of this questionnaire is presented in Appendix A and presents a sample of the threats that were rated; the full list of threats appears in Table 4-8. Questionnaire 1 is designed with a five-point Likert scale, from 1: very low risk to 5: very high risk and includes the following three purposes: (1) to validate the identified threats, (2) to explore more threats not identified from the literature review, and (3) to screen the importance of the identified threats for a furthermore in-depth analysis (to be performed using Questionnaire 2).

Selecting the right participants for your questionnaire, especially when seeking expert opinions, is crucial for obtaining valuable and reliable data. For our questionnaires non-probability sampling methods was utilised, starting with a Purposeful sampling (also known as judgment or subjective sampling) relying on our own judgment when choosing members of population to participate in the study. This method involved selecting participants based on their expertise or knowledge in the specific field, but who are also easy to reach and willing to participate. In order to obtain a high number of responses, These experts were requested to recommend other experts they are acquainted with, thereby initiating a snowball effect; this phenomenon is recognised as 'snowball sampling.' In fact, the same approach has been used for all questionnaires in this thesis.

In total, 100 copies of Questionnaire 1 were sent out to shipping companies, seafarers, port authorities, IMO experts, and academics. 38 replies have been received, of which 31 were complete (valid response rate: 31%) and have been used to prioritise the

importance of the assessed threats. The respondents' background is summarised in Table 4-7; 61.3% of them work in a shipping company, followed by 5.1% in the port authority and 13.63%, and rest of the respondents are in researchers in the maritime field and government organisation. In addition, 38.7% of them have 6 to 10 years of work experience.

Table 4-7: Questionnaire 1 Respondents' background

Organisation	Shipping company	19
	Port authorities	6
	Government organisation	2
	Academia	4
Work experience	Less than 5 years	9
	6 to 10 years	14
	11 to 15 years	3
	More than 16 years	5

Based on the experts' opinion, the top two threats are identified as "Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it" and "Employees do not follow company's cybersecurity process due to poor cybersecurity awareness"; both belong to the ''Human factor'' category. The third most concerned threat is "Connecting USB or removable media to computer without virus check", which belongs to the "Malware" category. The fourth and fifth also belong to this category and are "Accessing links from suspicious email" and "Connecting your infected USB or removable media to connect computers/navigation system", respectively.

The full results of Questionnaire 1 are presented in Table 4-8. The threats with relatively importance (see threats highlighted in green) were selected for a more thorough investigation through Questionnaire 2 and the application of novel FMEA-RBN methodology.

Table 4-8: The results of Questionnaire 1

Threats Category	Risk level	Threats of Maritime Cyber Security
Phishing	3.58	Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.)
	3.55	Downloading attached files from impersonation emails (e.g., bank, credit card company, insurance company, etc.)
	2.88	Accessing links from impersonation text messages (e.g., bank, credit card company, insurance company, etc.)
Malware	3.09	Downloading files (e.g., mp3, movie, games) from suspicious websites
	3.94	Accessing links from suspicious emails
	3.39	Downloading attached files from unknown emails
	4.03	Connecting USB or removable media to computer without virus check
	2.91	Accessing malicious advertising on websites
	3.82	Connecting your infected USB or removable media to connect computers/navigation systems
	3.58	DDoS attacks company's server system
Man in the middle attack	2.67	Using unsecured open Wi-Fi connections
	2.82	Using insecure Virtual Private Network (VPN)
	2.67	Applying weak WEP/WPA encryption on access points
	3.33	Providing personal/commercial information to friends/partners via open Wi-Fi connection
	3.36	Providing personal/commercial information to suspicious websites (e.g., illegal software/music/movie download websites)
Theft of credentials	3.48	Using automatically log in system (e.g., save your ID and password on websites)
	3.58	Using simple and easy to assume passwords
	3.33	Applying only single-factor authentication for login account system
	3.24	Providing personal information to a fake website (e.g., government website, etc.)
Human factor	4.15	Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it)
	3.70	Company does not set a proper cybersecurity process
	4.06	Employees do not follow company's cybersecurity process due to poor cybersecurity awareness
	3.76	Closing firewall due to careless operations or specific purpose
	3.55	Accessing suspicious links due to careless operations or specific purpose
Using outdated IT system	3.70	Using outdated version firewall and anti-virus software
	3.70	Using unpatched operating systems e.g., outdated window version
	3.27	Forgetting update software
	3.09	No planning applying up-to-date software

4.4.2 Results of FMEA-BRN

Questionnaire 2 (see Appendix B) was used to collect the DoB of the three parameters: likelihood of (L), consequence (C) and probability of failure of being undetected (P) of the selected threats identified through Questionnaire 1 (see Appendix A). The reason for using the DoB is that it considers respondents' uncertainty when answering questions.

In total, Questionnaire 2 has been sent to 100 maritime industry experts, who have rich experience in the maritime industry and are familiar with the topic of cyber-security. Respondents were asked to provide a percentage to each statement using five levels of linguistic terms; see Tables 3-2, 3-3, and 3-4 for the definitions of the levels of each parameter against each selected threat in Table 3-8. These parameters were presented in a table format, see Appendix B for a sample of the rating input table; the full list of threats presented to the experts is the one obtained by Questionnaire 1 and shown in Table 4-8.

For each parameter, the sum of the DoB of the five-level items should be 100%. For instance, a valid response would be that an expert believes that the likelihood of 'Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.)' is 30% High, and 70% Average, and the consequence is 40% Moderate and 60% Marginal, whereas for the probability of failure being undetected is 100 % Likely.

A total of 48 replies were collected, of which 44 replies were complete (valid response rate 44%). The respondents' background is summarised in Table 4-9; 77.27% of them work in a shipping company, followed by 9% in the port industry and 13.63% academic researchers in the maritime field. In addition, 46.46% of them have more than 10 years of experience.

Table 4-9: Questionnaire 2 Respondents' background

Organisation	Shipping company	34
	Port company	4
	Academia	6
Work experience	Less than 5 years	13
	6 to 10 years	11
	11 to 15 years	12
	More than 16 years	8

Assessment of 'Phishing' Threat Category

The result show that two threats are selected under the category of 'Phishing' based on the Questionnaire 1, including 'Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.)' and 'Downloading attached files from impersonation emails (e.g., bank, credit card company, insurance company, etc.)'.

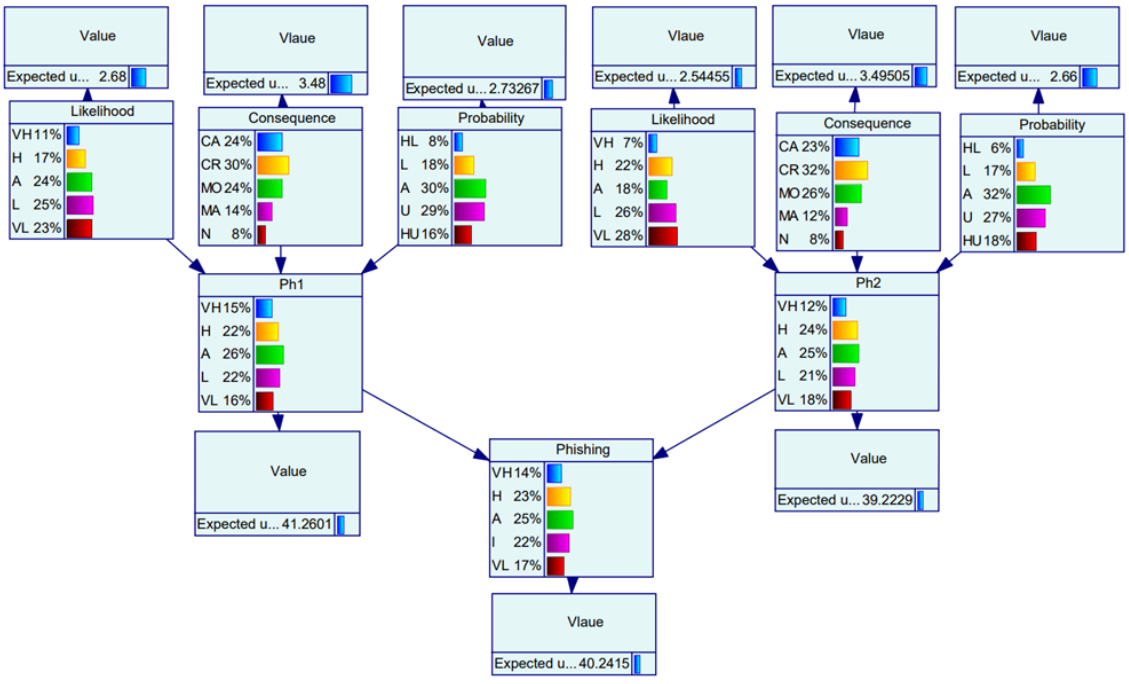


Figure 4-2: Result of the assessment of the 'Phishing' threat category

All figures are rounded up to a decimal point. In some cases, the sum of certain factors may exceed or fall below 100%. However, the actual calculated sum is 100%, so specify that it is not an incorrect calculation.

The results also show in Figure 4-2 that the value of likelihood of 'Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.)' (Ph1) is around 2.68, with 11% of Very High (VH), 17% of High (H), 24% of Average (A), 25% of Low (L), and 23% of Very Low (VL). Whereas the value of consequence is around 3.48, with 24% of Catastrophic (CA), 30% of Critical (CR), 24% of Moderate (MO), 14% of Marginal (MA), and 8% of Negligible (N). For the value of Probability of the failure being undetected is around 2.73, with 8% of Highly likely (HL), 18% of Likely (L), 30% of Average (A), 29% of Unlikely (U), and 16% of Highly Unlikely (HU). The overall risk value for 'Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.)' is around 41.26 after conducting BN calculation.

For the results of 'Downloading attached files from impersonation emails (e.g., bank, credit card company, insurance company, etc.)' (Ph2), the likelihood is around 2.54, with 7% of Very High (VH), 22% of High (H), 18% of Average (A), 26% of Low (L), and 28% of Very Low (VL). Whereas the value of consequence is around 3.49, with 23% of Catastrophic (CA), 32% of Critical (CR), 26% of Moderate (MO), 12% of Marginal (MA), and 8% of Negligible (N). For the value of Probability of the failure being undetected is around 2.66, with 6% of Highly likely (HL), 17% of Likely (L), 32% of Average (A), 27% of Unlikely (U), and 18% of Highly Unlikely (HU). The overall risk value for 'Downloading attached files from impersonation emails (e.g., bank, credit card company, insurance company, etc.)' is around 39.22 after conducting BN calculation. Finally, the overall risk value of 'Phishing' is 40.24.

Assessment 'Malware' Threat Category

The results show in Figure 4-3 that five threats are selected under the category of malware based on the results of the Questionnaire 1, including 'Accessing links from suspicious emails' (Mal1), 'Downloading attached files from unknown emails' (Mal2), 'Connecting USB or removable media to computer without virus check' (Mal3), 'Connecting your infected USB or removable media to connect computers/navigation systems' (Mal4), and 'DDoS attacks company's server system' (Mal5).

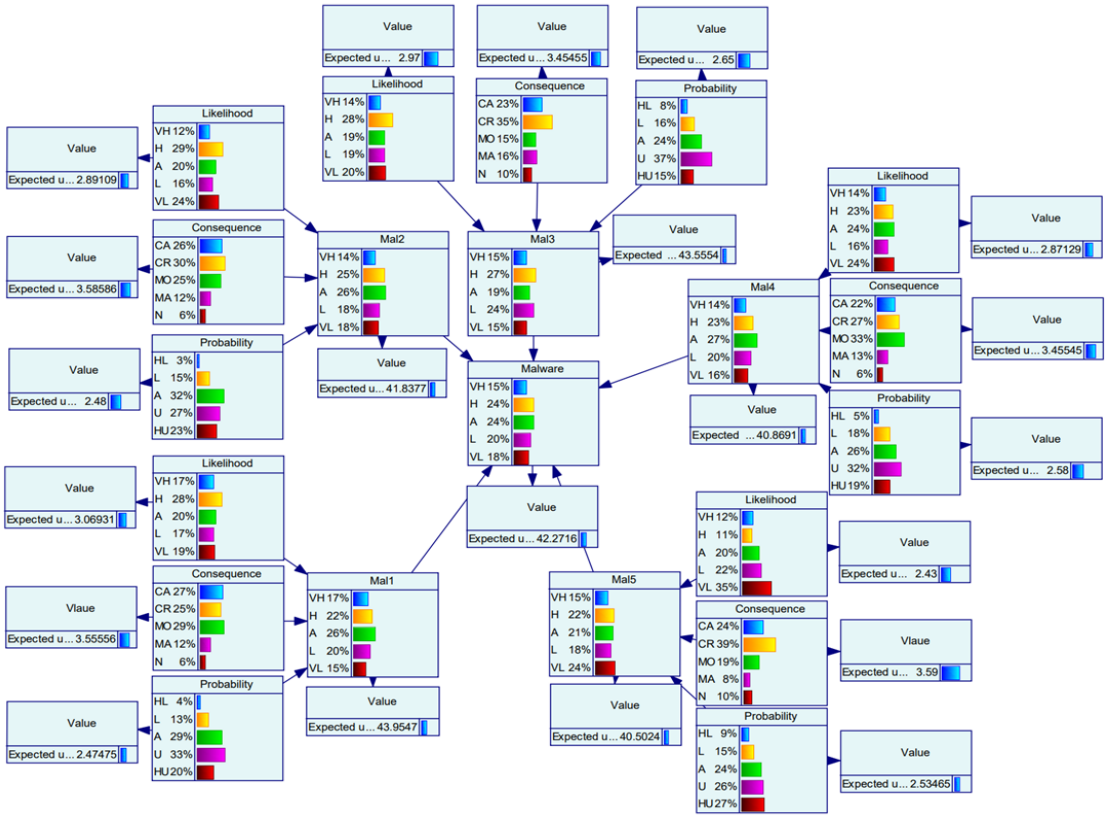


Figure 4-3: Result of the assessment of the 'Malware' threat category

The results also show that the value of likelihood of 'Accessing links from suspicious emails' is around 3.06, with 17% of Very High (VH), 28% of High (H), 20% of Average (A), 17% of Low (L), and 19% of Very Low (VL). Whereas the value of consequence is around 3.56, with 27% of Catastrophic (CA), 25% of Critical (CR), 29% of Moderate (MO), 12% of Marginal (MA), and 6% of Negligible (N). For the value of Probability of the failure being undetected is around 2.47, with 4% of Highly likely (HL), 13% of Likely (L), 29% of Average (A), 33% of Unlikely (U), and 20% of Highly Unlikely (HU). The overall risk value for 'Accessing links from suspicious emails' is around 43.95 after conducting BN calculation.

For the results of 'Downloading attached files from unknown emails', the likelihood is around 2.89, with 12% of Very High (VH), 29% of High (H), 20% of Average (A), 16% of Low (L), and 24% of Very Low (VL). Whereas the value of consequence is around 3.59, with 26% of Catastrophic (CA), 30% of Critical (CR), 25% of Moderate (MO), 12% of Marginal (MA), and 6% of Negligible (N). For the value of Probability of the failure being

undetected is around 2.48, with 3% of Highly likely (HL), 15% of Likely (L), 32% of Average (A), 27% of Unlikely (U), and 23% of Highly Unlikely (HU). The overall risk value for 'Downloading attached files from unknown emails' is around 41.84 after conducting BN calculation.

For the results of 'Connecting USB or removable media to computer without virus check', the likelihood is around 2.97, with 14% of Very High (VH), 28% of High (H), 19% of Average (A), 19% of Low (L), and 20% of Very Low (VL). Whereas the value of consequence is around 3.45, with 23% of Catastrophic (CA), 35% of Critical (CR), 15% of Moderate (MO), 16% of Marginal (MA), and 10% of Negligible (N). For the value of Probability of the failure being undetected is around 2.65, with 8% of Highly likely (HL), 16% of Likely (L), 24% of Average (A), 37% of Unlikely (U), and 15% of Highly Unlikely (HU). The overall risk value for 'Connecting USB or removable media to computer without virus check' is around 43.56 after conducting BN calculation.

For the results of 'Connecting your infected USB or removable media to connect computers/ navigation systems', the likelihood is around 2.87, with 14% of Very High (VH), 23% of High (H), 24% of Average (A), 16% of Low (L), and 24% of Very Low (VL). Whereas the value of consequence is around 3.46, with 22% of Catastrophic (CA), 27% of Critical (CR), 33% of Moderate (MO), 13% of Marginal (MA), and 16% of Negligible (N). For the value of Probability of the failure being undetected is around 2.58, with 5% of Highly likely (HL), 18% of Likely (L), 26% of Average (A), 32% of Unlikely (U), and 19% of Highly Unlikely (HU). The overall risk value for 'Connecting your infected USB or removable media to connect computers/ navigation systems' is around 40.87 after conducting BN calculation.

For the results of 'DDoS attacks company's server system', the likelihood is around 2.43, with 12% of Very High (VH), 11% of High (H), 20% of Average (A), 22% of Low (L), and 35% of Very Low (VL). Whereas the value of consequence is around 3.59, with 24% of Catastrophic (CA), 39% of Critical (CR), 19% of Moderate (MO), 8% of Marginal (MA), and 10% of Negligible (N). For the value of Probability of the failure being undetected is

around 2.53, with 9% of Highly likely (HL), 15% of Likely (L), 24% of Average (A), 26% of Unlikely (U), and 27% of Highly Unlikely (HU). The overall risk value for 'DDoS attacks company's server system' is around 40.5 after conducting BN calculation. Finally, the overall risk value of 'Malware' is 42.27.

Assessment of 'Man in the middle attack' Threat Category

The results show in Figure 4-4 that two threats are selected under the category of Man in the middle attack based on the results of the Questionnaire 1, including 'Providing personal/commercial information to friends/partners via open Wi-Fi connection' (MITM1), and 'Providing personal/commercial information to suspicious websites (e.g., illegal software/music/movie download websites)' (MITM2).

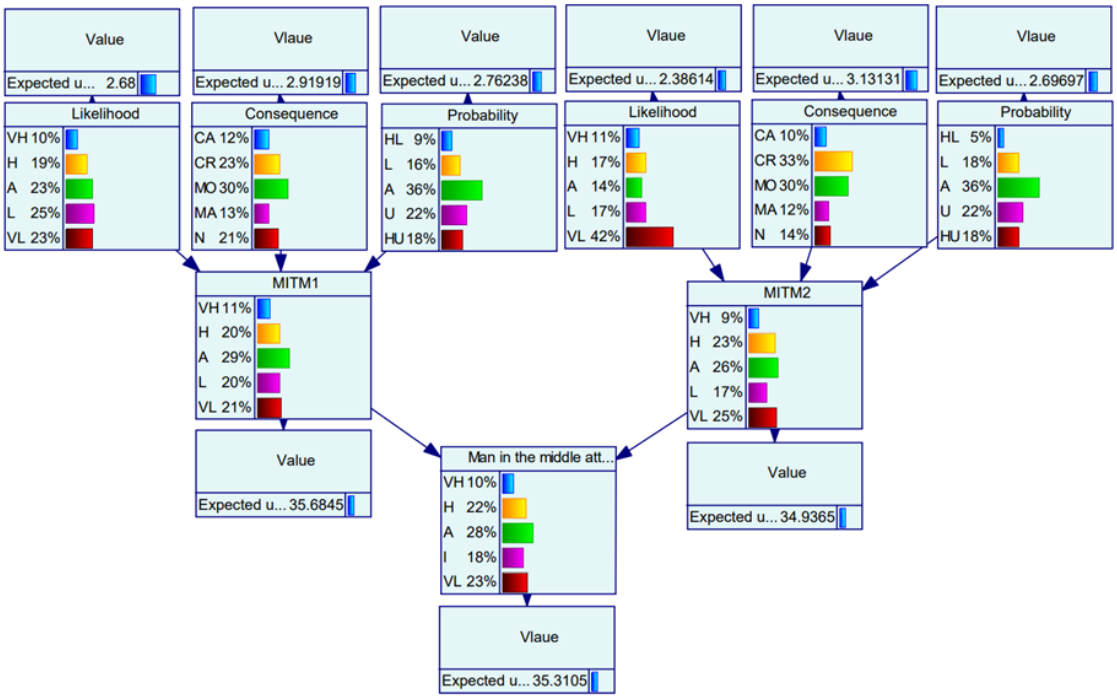


Figure 4-4: Result of the assessment of the 'Man in the middle attack' threat category

The results also present that the value of likelihood of 'Providing personal/commercial information to friends/partners via open Wi-Fi connection' is around 2.68, with 10% of Very High (VH), 19% of High (H), 23% of Average (A), 25% of Low (L), and 23% of Very Low (VL). Whereas the value of consequence is around 2.92, with 12% of Catastrophic (CA), 23% of Critical (CR), 30% of Moderate (MO), 13% of Marginal (MA), and 21% of

Negligible (N). For the value of Probability of the failure being undetected is around 2.76, with 9% of Highly likely (HL), 16% of Likely (L), 36% of Average (A), 22% of Unlikely (U), and 18% of Highly Unlikely (HU). The overall risk value for 'Providing personal/commercial information to friends/partners via open Wi-Fi connection' is around 35.68 after conducting BN calculation.

For the results of 'Providing personal/commercial information to suspicious websites (e.g., illegal software/music/movie download websites)', the likelihood is around 2.39, with 11% of Very High (VH), 17% of High (H), 14% of Average (A), 17% of Low (L), and 42% of Very Low (VL). Whereas the value of consequence is around 3.13, with 10% of Catastrophic (CA), 33% of Critical (CR), 30% of Moderate (MO), 12% of Marginal (MA), and 14% of Negligible (N). For the value of Probability of the failure being undetected is around 2.70, with 5% of Highly likely (HL), 18% of Likely (L), 36% of Average (A), 22% of Unlikely (U), and 18% of Highly Unlikely (HU). The overall risk value for 'Providing personal/commercial information to suspicious websites (e.g., illegal software/music/movie download websites)' is around 34.94 after conducting BN calculation. Finally, the overall risk value of 'Man in the middle attack' is 35.31.

Assessment of 'Theft of credential' Threat Category

The results show in Figure 4-5 that four threats are selected under the category of 'Theft of credential' based on the results of the Questionnaire 1, including 'Using automatically log in system (TC1)' (save password in Figure 7), 'Using simple and easy to assume password' (TC2), 'Applying only single factor authentication for log in account system' (TC3), and 'Providing personal information to a fake website (e.g., government website, etc.)' (TC4).

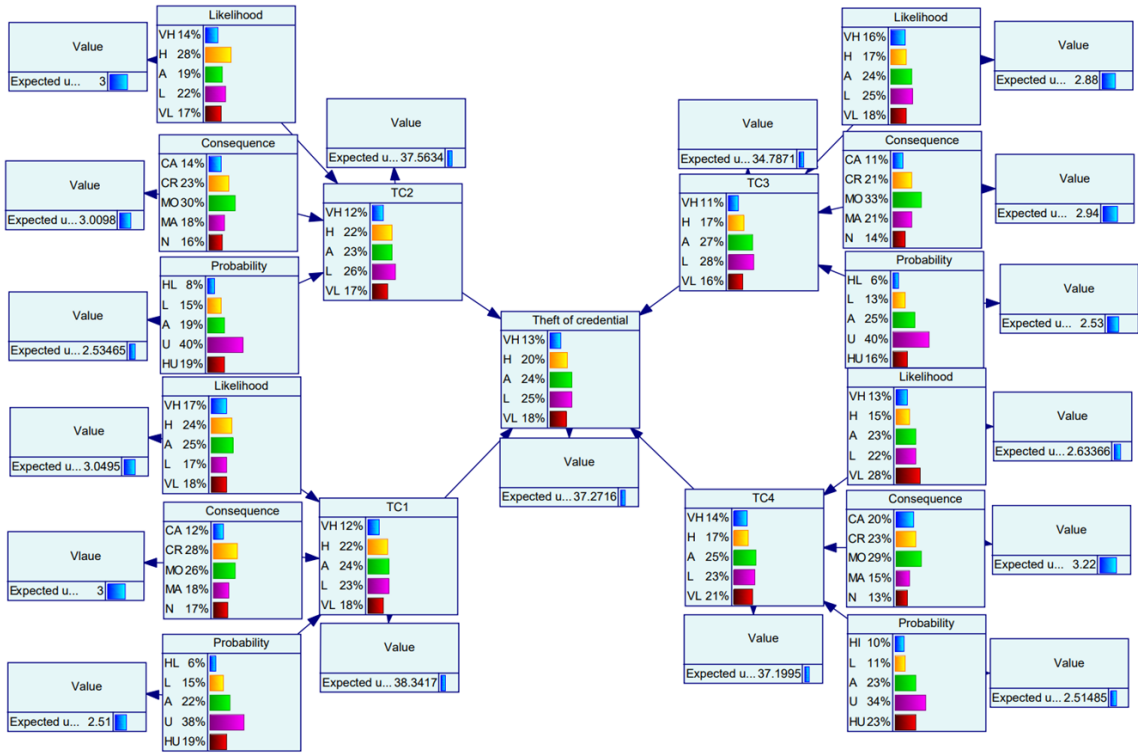


Figure 4-5: Result of the assessment of the 'Theft of credential' threat category

The results also show that the value of likelihood of 'Using automatically log in system (e.g., save your ID and password on website)' is around 3.04, with 17% of Very High (VH), 24% of High (H), 25% of Average (A), 17% of Low (L), and 18% of Very Low (VL). Whereas the value of consequence is around 3, with 12% of Catastrophic (CA), 28% of Critical (CR), 26% of Moderate (MO), 18% of Marginal (MA), and 17% of Negligible (N). For the value of Probability of the failure being undetected is around 2.51, with 6% of Highly likely (HL), 15% of Likely (L), 22% of Average (A), 38% of Unlikely (U), and 19% of Highly Unlikely (HU). The overall risk value for 'Using automatically log in system (e.g., save your ID and password on website)' is around 38.34 after conducting BN calculation.

For the results of 'Using simple and easy to assume password', the likelihood is around 3, with 14% of Very High (VH), 28% of High (H), 19% of Average (A), 22% of Low (L), and 17% of Very Low (VL). Whereas the value of consequence is around 3.01, with 14% of Catastrophic (CA), 23% of Critical (CR), 30% of Moderate (MO), 18% of Marginal (MA), and 16% of Negligible (N). For the value of Probability of the failure being undetected is around 2.53, with 8% of Highly likely (HL), 15% of Likely (L), 19% of Average (A), 40% of

Unlikely (U), and 19% of Highly Unlikely (HU). The overall risk value for 'Using simple and easy to assume password' is around 37.56 after conducting BN calculation.

For the results of 'Applying only single factor authentication for log in account system', the likelihood is around 2.88, with 16% of Very High (VH), 17% of High (H), 24% of Average (A), 25% of Low (L), and 18% of Very Low (VL). Whereas the value of consequence is around 2.94, with 11% of Catastrophic (CA), 21% of Critical (CR), 33% of Moderate (MO), 21% of Marginal (MA), and 14% of Negligible (N). For the value of Probability of the failure being undetected is around 2.53, with 6% of Highly likely (HL), 13% of Likely (L), 25% of Average (A), 40% of Unlikely (U), and 16% of Highly Unlikely (HU). The overall risk value for 'Applying only single factor authentication for log in account system' is around 34.79 after conducting BN calculation.

For the results of 'Providing personal information to a fake website (e.g., government website, etc.)', the likelihood is around 2.63, with 13% of Very High (VH), 15% of High (H), 23% of Average (A), 22% of Low (L), and 28% of Very Low (VL). Whereas the value of consequence is around 3.22, with 20% of Catastrophic (CA), 23% of Critical (CR), 29% of Moderate (MO), 15% of Marginal (MA), and 13% of Negligible (N). For the value of Probability of the failure being undetected is around 2.51, with 10% of Highly likely (HL), 11% of Likely (L), 23% of Average (A), 34% of Unlikely (U), and 23% of Highly Unlikely (HU). The overall risk value for 'Providing personal information to a fake website (e.g., government website, etc.)' is around 37.2 after conducting BN calculation. Finally, the overall risk value of 'Theft of credential' is 37.27.

Assessment of 'Human factor' Threat Category

The results show in Figure 4-6 that five threats are selected under the category of human factor based on the results of the Questionnaire 1, including 'Lacking knowledge of cybersecurity (i.e. facing a new situation and do not know how to deal with it)' (HF1), 'Company does not set a proper cybersecurity process' (HF2), 'Employees do not follow company's cybersecurity process due to poor cybersecurity awareness' (HF3), 'Closing

firewall due to careless operations or specific purpose' (HF4), and 'Accessing suspicious links due to careless operations or specific purpose' (HF5).

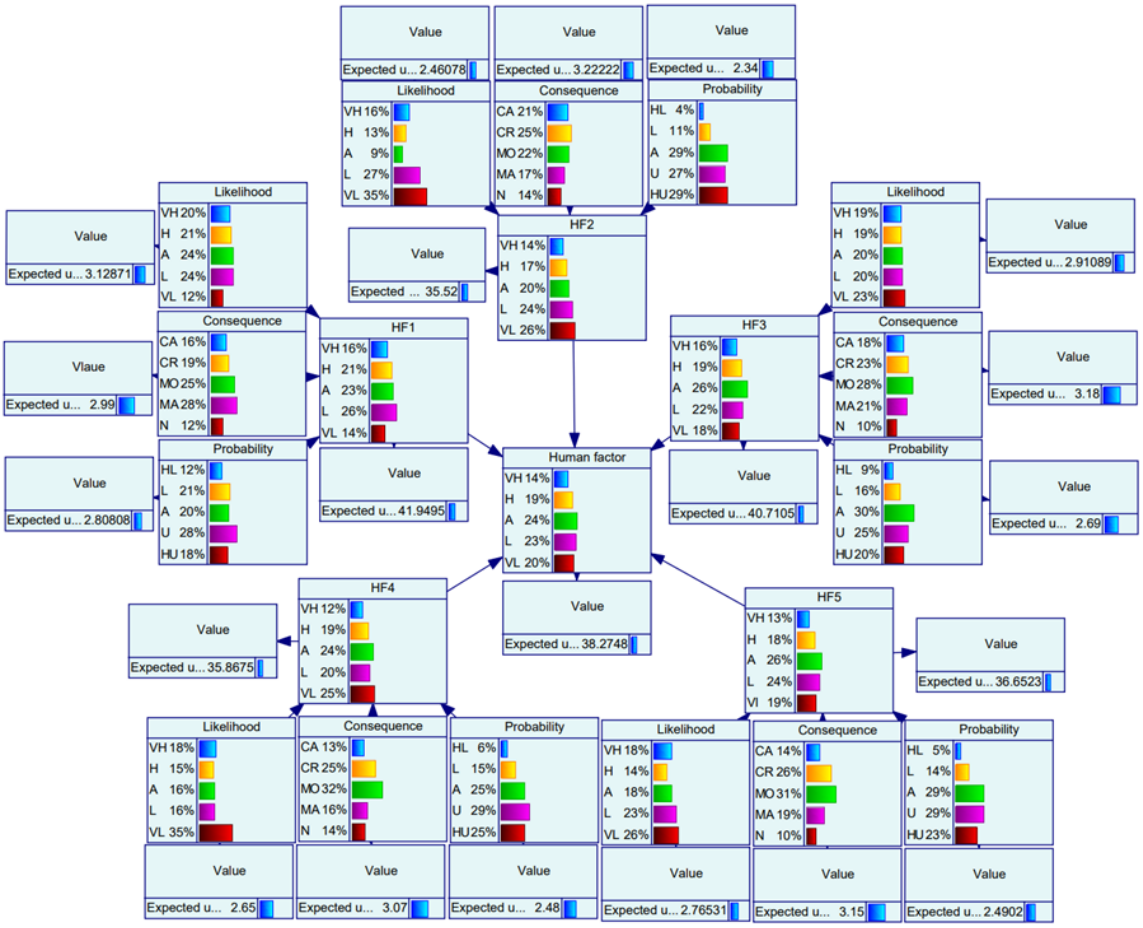


Figure 4-6: Result of the assessment of the 'Human factor' threat category

The results also show that the value of likelihood of 'Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it)' is around 3.12, with 20% of Very High (VH), 21% of High (H), 24% of Average (A), 24% of Low (L), and 12% of Very Low (VL). Whereas the value of consequence is around 2.99, with 16% of Catastrophic (CA), 19% of Critical (CR), 25% of Moderate (MO), 28% of Marginal (MA), and 12% of Negligible (N). For the value of Probability of the failure being undetected is around 2.81, with 12% of Highly likely (HL), 21% of Likely (L), 20% of Average (A), 28% of Unlikely (U), and 18% of Highly Unlikely (HU). The overall risk value for 'Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it)' is around 41.95 after conducting BN calculation.

For the results of 'Company does not set a proper cybersecurity process', the likelihood is around 2.46, with 16% of Very High (VH), 13% of High (H), 9% of Average (A), 27% of Low (L), and 35% of Very Low (VL). Whereas the value of consequence is around 3.22, with 21% of Catastrophic (CA), 25% of Critical (CR), 22% of Moderate (MO), 17% of Marginal (MA), and 14% of Negligible (N). For the value of Probability of the failure being undetected is around 2.34, with 4% of Highly likely (HL), 11% of Likely (L), 29% of Average (A), 27% of Unlikely (U), and 29% of Highly Unlikely (HU). The overall risk value for 'Company does not set a proper cybersecurity process' is around 35.52 after conducting BN calculation.

For the results of 'Employees do not follow company's cybersecurity process due to poor cybersecurity awareness', the likelihood is around 2.91, with 19% of Very High (VH), 19% of High (H), 20% of Average (A), 20% of Low (L), and 23% of Very Low (VL). Whereas the value of consequence is around 3.18, with 18% of Catastrophic (CA), 23% of Critical (CR), 28% of Moderate (MO), 21% of Marginal (MA), and 10% of Negligible (N). For the value of Probability of the failure being undetected is around 2.69, with 9% of Highly likely (HL), 16% of Likely (L), 30% of Average (A), 25% of Unlikely (U), and 20% of Highly Unlikely (HU). The overall risk value for 'Employees do not follow company's cybersecurity process due to poor cybersecurity awareness' is around 40.71 after conducting BN calculation.

For the results of 'Closing firewall due to careless operations or specific purpose', the likelihood is around 2.65, with 18% of Very High (VH), 15% of High (H), 16% of Average (A), 16% of Low (L), and 35% of Very Low (VL). Whereas the value of consequence is around 3.07, with 13% of Catastrophic (CA), 25% of Critical (CR), 32% of Moderate (MO), 16% of Marginal (MA), and 14% of Negligible (N). For the value of Probability of the failure being undetected is around 2.48, with 6% of Highly likely (HL), 15% of Likely (L), 25% of Average (A), 29% of Unlikely (U), and 25% of Highly Unlikely (HU). The overall risk value for 'Closing firewall due to careless operations or specific purpose' is around 35.87 after conducting BN calculation.

For the results of 'Accessing suspicious links due to careless operations or specific purpose', the likelihood is around 2.76, with 18% of Very High (VH), 14% of High (H), 18% of Average (A), 23% of Low (L), and 26% of Very Low (VL). Whereas the value of consequence is around 3.15, with 14% of Catastrophic (CA), 26% of Critical (CR), 31% of Moderate (MO), 19% of Marginal (MA), and 10% of Negligible (N). For the value of Probability of the failure being undetected is around 2.49, with 5% of Highly likely (HL), 14% of Likely (L), 29% of Average (A), 29% of Unlikely (U), and 23% of Highly Unlikely (HU). The overall risk value for 'Accessing suspicious links due to careless operations or specific purpose' is around 36.65 after conducting BN calculation. Finally, the overall risk value of 'Human factor' is 38.27.

Assessment of 'Using outdated IT system' Threat Category

The results in Figure 4-7 show that three threats are selected under the category of 'Using outdated IT system' based on the results of the Questionnaire 1, including 'Using outdated version firewall and anti-virus software' (IT1), 'Using unpatched operating system e.g., outdated window version' (IT2), and 'Forgetting update software' (IT3).

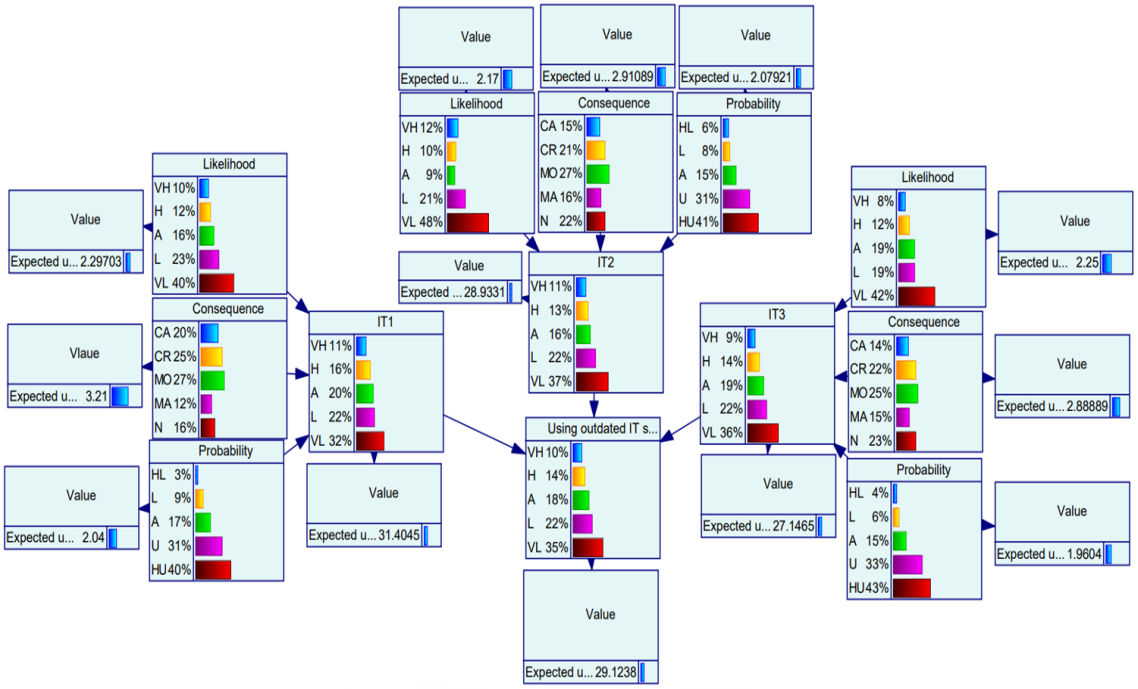


Figure 4-7: Result of the assessment of the 'Using outdated IT system' threat category

The results also show that the value of likelihood of 'Using outdated version firewall and anti-virus software' is around 2.3, with 10% of Very High (VH), 12% of High (H), 16% of Average (A), 23% of Low (L), and 40% of Very Low (VL). Whereas the value of consequence is around 3.21, with 20% of Catastrophic (CA), 25% of Critical (CR), 27% of Moderate (MO), 12% of Marginal (MA), and 16% of Negligible (N). For the value of Probability of the failure being undetected is around 2.04, with 3% of Highly likely (HL), 9% of Likely (L), 17% of Average (A), 31% of Unlikely (U), and 40% of Highly Unlikely (HU). The overall risk value for 'Using outdated version firewall and anti-virus software' is around 31.40 after conducting BN calculation.

For the results of 'Using unpatched operating system e.g., outdated window version', the likelihood is around 2.17, with 12% of Very High (VH), 10% of High (H), 9% of Average (A), 21% of Low (L), and 48% of Very Low (VL). Whereas the value of consequence is around 2.91, with 15% of Catastrophic (CA), 21% of Critical (CR), 27% of Moderate (MO), 16% of Marginal (MA), and 22% of Negligible (N). For the value of Probability of the failure being undetected is around 2.07, with 6% of Highly likely (HL), 8% of Likely (L), 15% of Average (A), 31% of Unlikely (U), and 41% of Highly Unlikely (HU). The overall risk value for 'Using unpatched operating system e.g., outdated window version' is around 28.93 after conducting BN calculation.

For the results of 'Forgetting update software', the likelihood is around 2.25, with 8% of Very High (VH), 12% of High (H), 19% of Average (A), 19% of Low (L), and 42% of Very Low (VL). Whereas the value of consequence is around 2.89, with 14% of Catastrophic (CA), 22% of Critical (CR), 25% of Moderate (MO), 15% of Marginal (MA), and 23% of Negligible (N). For the value of Probability of the failure being undetected is around 1.96, with 4% of Highly likely (HL), 6% of Likely (L), 15% of Average (A), 33% of Unlikely (U), and 43% of Highly Unlikely (HU). The overall risk value for 'Forgetting update software' is around 27.15 after conducting BN calculation. Finally, the overall risk value of 'Using outdated IT system' is 29.12.

The results show that the threat category of ‘Malware’ has the highest risk value (risk value 42.27), followed by ‘Phishing’ (risk value: 40.24), and ‘Human factor’ (risk value: 38.27); whereas the least important threat category is that of ‘Using outdated IT’ (risk value: 29.12).

Overall, the top three threats include ‘Accessing links from suspicious emails’ (Mal1, risk value: 43.95), ‘Connecting USB or removable media to a computer without virus check’ (Mal3, risk value: 43.56), and ‘Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it)’ (risk value: 41.95); whereas the least three important threats that contribute to maritime cybersecurity risk are ‘Forgetting to update software’ (risk value: 27.15), ‘Using unpatched operating system e.g., outdated window version’(risk value: 28.93), and ‘Using outdated version firewall and anti-virus software’ (risk value: 31.4). The summary of the results from Questionnaire 2 are shown in Table 4-10.

Table 4-10: Risk values of threat categories and threats from Questionnaire 2

Threat category	Category value	Threat	Threat value
Phishing	40.24	Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.) (Ph1)	41.26
		Downloading attached files from impersonation emails (e.g., bank, credit card company, insurance company, etc.) (Ph2)	39.22
Malware	42.27	Accessing links from suspicious emails (Mal1)	43.95
		Downloading attached files from unknown emails (Mal2)	41.84
		Connecting USB or removable media to a computer without virus check (Mal3)	43.56
		Connecting your infected USB or removable media to connect computers/ navigation systems (Mal4)	40.87
		DDoS attacks company's server system (Mal5)	40.5
Man in the middle attack	35.31	Providing personal/commercial information to friends/partners via open Wi-Fi connection (MITM1)	35.68
		Providing personal/commercial information to suspicious websites (e.g., illegal software/music/movie download websites) (MITM2)	34.94
Theft of credential	37.27	Using automatically log in system (e.g., save your ID and password on website) (TC1)	38.34
		Using simple and easy to assume passwords (TC2)	37.56
		Applying only single-factor authentication for login account system (TC3)	34.79
		Providing personal information to a fake website (e.g., government website, etc.) (TC4)	37.2
Human factor	38.27	Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it) (HF1)	41.95
		Company does not set a proper cybersecurity process (HF2)	35.52
		Employees do not follow company's cybersecurity process due to poor cybersecurity awareness (HF3)	40.71
		Closing firewall due to careless operations or specific purpose (HF4)	35.87
		Accessing suspicious links due to careless operations or specific purpose (HF5)	36.65
Using outdated IT system	29.12	Using outdated version firewall and anti-virus software (IT1)	31.4
		Using unpatched operating system e.g., outdated window version (IT2)	28.93
		Forgetting update software (IT3)	27.15

Note: red colour refers to risk value more than 40; yellow colour refers to risk value between 30 and 40; green colour refers to risk value less than 30.

4.4.3 Validation and Sensitivity Analysis

The BN-based model requires validation to check whether the model is robust and to ensure the reliability of the results. An in-person meeting is also conducted to have a validation of the rationality of the proposed model with three experts from the maritime industry:

(1) A captain with more than 20 years of work experience who has a number of experiences dealing with cyberattacks on board

(2) An IT manager of a container shipping company with more than 15 years of work experience

(3) A maritime-related research scholar with more than 15 years of work experience.

All three experts have much experience on the topic "maritime cybersecurity". For example, they all have more than 15 years' work experience and they all have professional knowledge related to the maritime industry and cybersecurity. In the meeting, all experts agreed with the rationale for the framework, as well as its elements and structure. Both questionnaires have also been validated by the three experts.

In order to carry out the further validation of the model, a comprehensive set of data related to cybersecurity incidents needs to be collected, which is impractical at this stage of the research. Due to lack of comprehensive data, this study's validation is performed through a sensitivity analysis in line with Jones et al. (2010). Meanwhile, both questionnaires lead to similar results as it has been illustrated above, i.e., the top three threats identified from Questionnaire 2 are among the top five threats identified using Questionnaire 1. In addition, a sensitivity analysis has been carried out in line with similar studies, see for example Yang et al. (2008), Yu et al. (2020) and Chang et al. (2021). The used software implements a simple algorithm; given a set of target nodes, a complete set of derivatives of the posterior probability distributions over the target nodes (in this case, the overall risk) can be calculated. If the derivative is large for a parameter, a small change in it may lead to a large change in the posteriors of the targets. The bar shows the changes of the overall risk from the change of each threat.

The sensitivity analysis is to investigate the impact of various threats on the overall risk. Two extreme results are listed for illustration purposes: the overall risk being 'very high' (Figure 4-8) and 'very low' (Figure 4-9). In Figure 3-8, the value of Ph2 varies between 0.1163 and 0.1993, implying the 'very high' of the overall risk will increase to 0.1993 when setting Ph2 to 100% 'very high' (keeping the other threats the same); whereas the 'very high' of the overall risk will decrease to 0.1163 when setting Ph2 to 0% 'very high'. Therefore, Ph2 has the highest impact on the overall risk among all threats. Meanwhile, Mal3 (the last bar in Figure 3-8) shows the lowest impact on the overall risk. In this process, the setting of Ph2 is changed from 0% 'very high' to 100% 'very high' with a step of 10%. The impact of every change to the target node 'risk' is consistently increased, which is in line with Axiom 1. In a similar way, the impact levels of the threats are also in good harmony with their importance. It proves the model against Axiom 2.

Figure 4-8 illustrates that in the context of 'very high' (VH) overall risk, 'Downloading attached files from impersonation emails (e.g., bank, credit card company, insurance company, etc.) (Ph2) has the most significant impact on the overall risk in total. In contrast, the one with the lowest impact on the overall risk is 'Connecting USB or removable media to a computer without virus check' (Mal3) in the bottom of the figure, which indicates that this kind of mistake will result in a relatively low impact compared to the highly ranked threats. The most positive impact one is 'Providing personal/commercial information to suspicious websites (e.g., illegal software/music/movie download websites)' (the green part of MITM2). However, the most negative impact one is 'Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.) (the red part of Ph1).

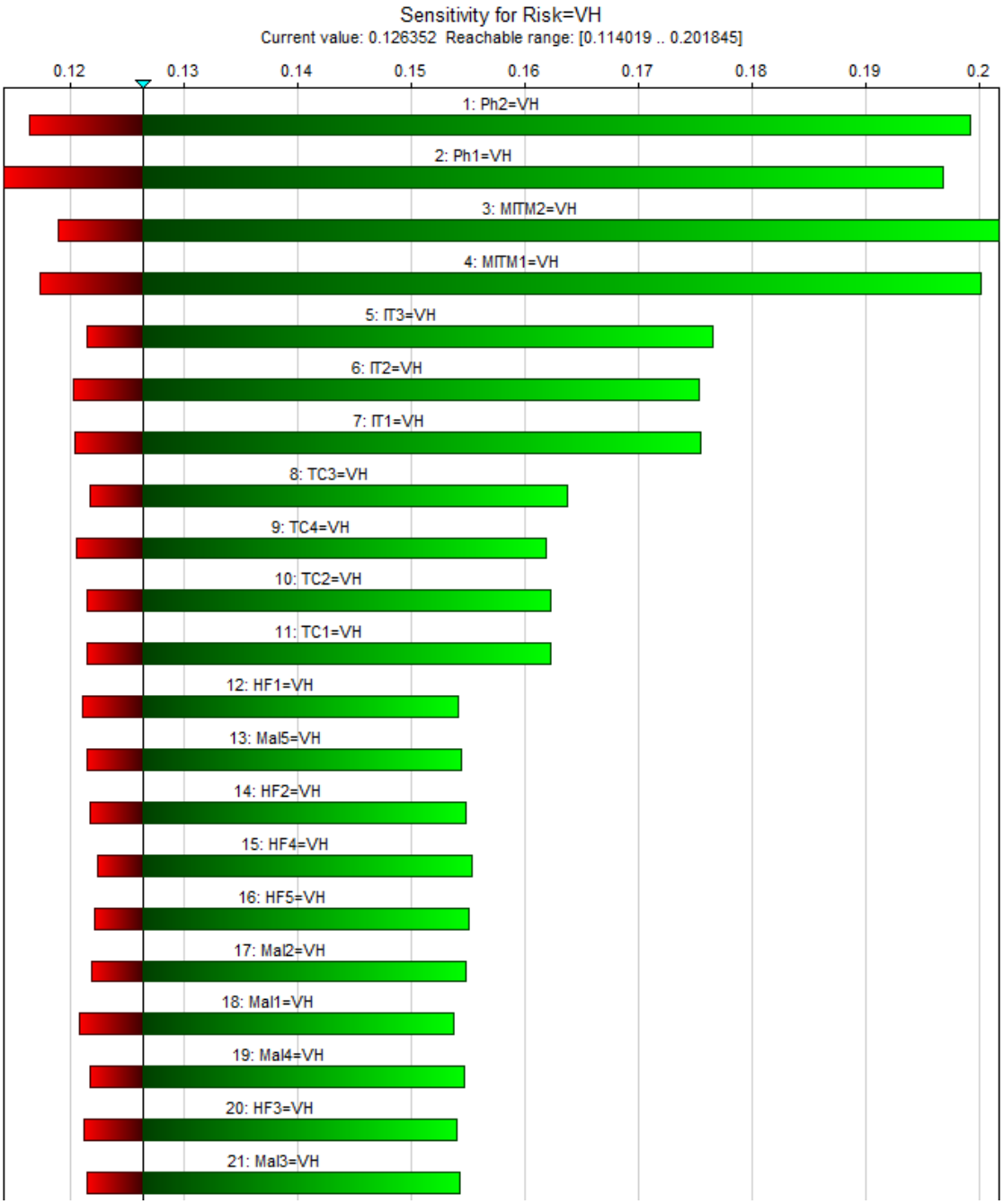


Figure 4-8: Sensitivity analysis in very high overall risk

Figure 4-9 shows two critical situations influencing the overall risk of maritime cybersecurity: (a) 'Not providing personal/commercial information to suspicious websites as opposed to providing personal/commercial information to suspicious websites (e.g., illegal software/music/movie download websites)' would significantly decrease the overall risk to a 'very low' level (see the red part of MITM2) and (b) 'Accessing links from impersonation emails (e.g., bank, credit card company, insurance

company, etc.)' will largely increase the overall risk (the green part of PH1). In addition, Figure 4-9 also depicts that 'Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it)' and 'Accessing links from suspicious emails' should not be considered in a very low overall maritime cybersecurity risk as it has limited positive impact (the green part of HF1 and Mal1).

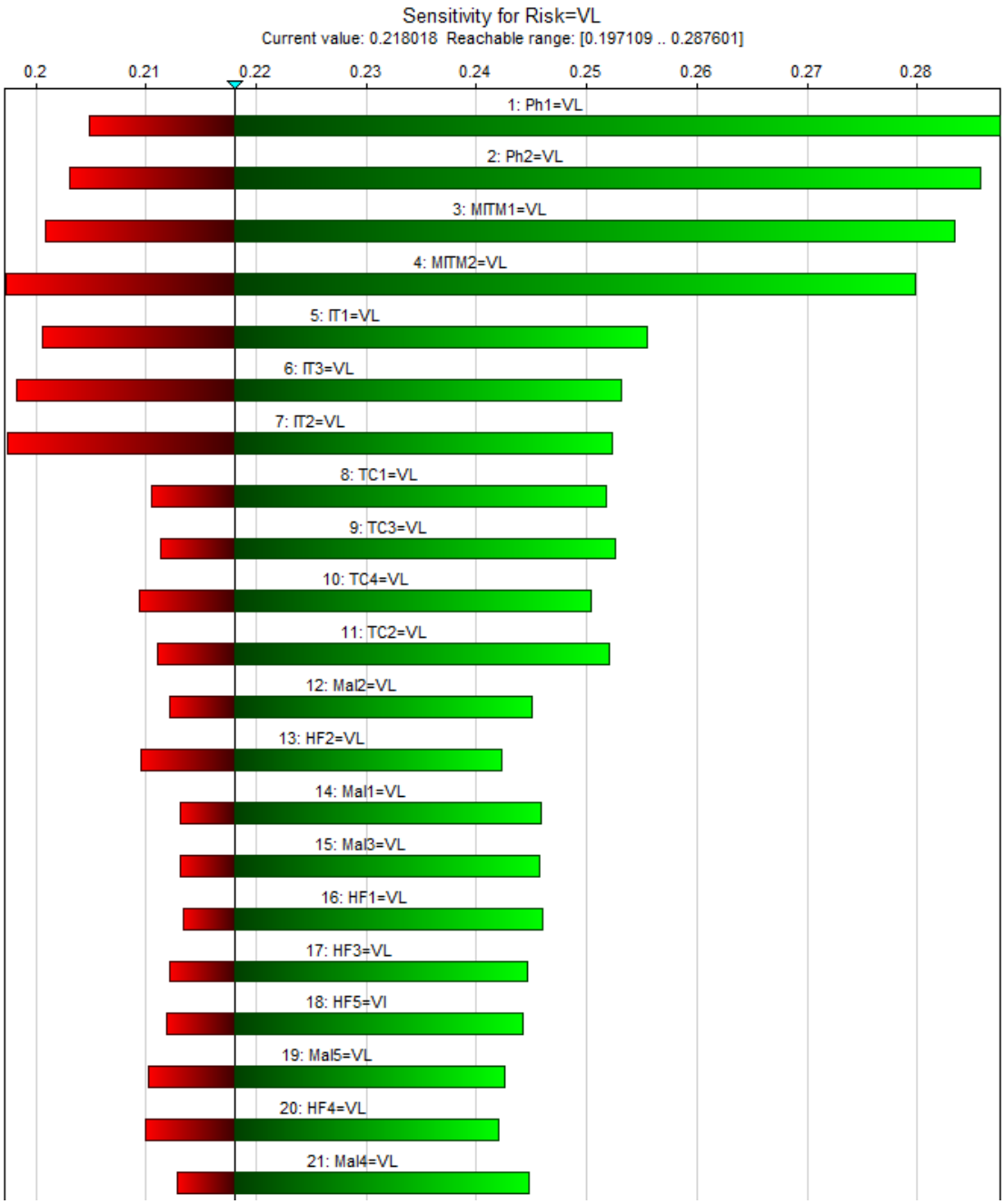


Figure 4-9: Sensitivity analysis in very low overall risk

Although not in the top five threats, as it can be seen in Figures 3-8 and 3-9, Ph1, Ph2, MTM1, and MTM2 have revealed significant impact on the overall risk. By controlling these threats, the overall risk can be significantly reduced, because of their high impact and sensitivity.

4.5 Discussion

The results in Section 3.4 show that 'Malware' is the most important cybersecurity risk category. This indicates that the maritime industry should try to identify some measures either to mitigate the impacts of the consequences of malware or to preventing them by reducing the likelihood or probability of the threat being undetected. However, the top values are just in the middle between U_{R3} (27) and U_{R4} (64), which indicates that most of the respondents feel that cyber threats do not significantly impact the maritime industry. On the other side, the lowest cyber threat category is 'Using outdated IT systems' with a value very close to U_{R3} (27), which refers to that the respondents do not think this is an important factor that contributes to the maritime cybersecurity risk. By checking the aggregated data, it is found that the likelihood of the three cyber threats is the lowest among the three parameters, which implies that most of the respondents believe that their companies have updated the IT to the latest version to protest the damage from the cyberattacks.

There are eight threats that have values above 40; the top three threats are 'Accessing links from suspicious emails (Mal1)', 'Connecting USB or removable media to a computer without virus check (Mal3)', and 'Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it) (HF1)'. The top two cyber threats belong to the category of 'Malware', which has been identified as the top cyber-risk category and illustrates the importance of addressing this area. Sea crew and company staff might attempt to operate navigational or company's IT systems in convenient ways, which might cause more cyber vulnerability and a higher likelihood to be cyberattacked. However, these top three cyber threats can all be controlled through increased cybersecurity awareness, which could be gained through regular training and education.

4.5.1 Practical Implications of the Findings

This chapter presents a novel risk assessment of maritime cyber threats; it analyses the identified cyber threats, analyses their risks for their prioritisation. The next step in managing cyber threats is to focus on those threats that are associated with unacceptable risk and identify cost- effective measures to manage them. To that extent, the findings provide a list of top threats – that is the areas where efforts should be focused on. In light of this, some countermeasures that could address the top threats are put forward. This analysis provides the foundation for the development of a new decision-making method to realise the optimal selection of cost-effective security measures. Some of the key areas are the following:

Education, training, and awareness are very important. Experts feel that 'Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it) (HF1)' is one of the top threats. Training and education of people about the risks, particularly awareness improvement is essential. It is to impart fundamental knowledge and tools. Regular training will help attain awareness. Many studies have suggested that training and educating seafarers and staff is an effective method to improve maritime cybersecurity (Jones et al., 2016; Bolbot et al., 2020; Kanwal et al., 2022). They suggested that seafarers should be trained to deal with cyber incidents manually to protect the system and to reduce damage to equipment. At the same time, efforts on enhancing cybersecurity awareness have been witnessed with growing importance. BIMCO (2018) argued that the maritime industry lacks a cyber-awareness culture and governance, and this could increase its vulnerability and, thus, because more cyberattack incidents. Furthermore, shipping companies are required to develop cybersecurity management systems to urge cybersecurity awareness (IMO, 2017b).

To address human errors in cybersecurity, software can help reduce threats. 'Accessing links from suspicious emails (Mal1)', 'Downloading attached files from unknown emails (Mal2)' and 'Connecting USB or removable media to a computer without virus check (Mal3)' have been identified as top threats in this study. These could be well prevented by software. For example, installing and regularly updating anti-virus software have

shown significant effectiveness in reducing cybersecurity risks. This can stop malicious software from being downloaded, and also from being executed. This is supported by the recommendation of BIMCO (2018) that an anti-virus software should be installed on all work-related computers on board to reduce the possibility of cyberattacks. It also reports that the number of maritime cyber incidents increased notably due to lack of software maintenance and patching. It is unavoidable to encounter various viruses and malicious software with the development of advanced technologies applied in the maritime industry. Shipping companies should pay particular attention to updating and upgrading their IT and OT systems to deal with the high-ranked threats identified in this research and, hence, to ensure their competitiveness.

4.6 Conclusions

This chapter conducts a risk assessment of maritime cybersecurity. Maritime cyber threats are first identified through thorough literature research. In total, 28 maritime cyber threats are identified. These threats can be categorised into six groups, including 'Phishing,' 'Malware,' 'Man in the Middle Attack,' 'Theft of Credentials,' 'Human Factors,' and 'Use of Outdated IT Systems.

To assess these threats, two sets of questionnaires are distributed to collect opinions from maritime experts. Questionnaire 1 (Appendix A), which employs a five-point Likert scale, is used to validate the identified threats, explore any additional threats not identified in the literature review, and gauge the overall importance of these threats. In total, 100 questionnaires were distributed, and 31 responses were received. Based on the mean values assigned to the threats, 21 threats with relatively higher mean values are selected for inclusion in Questionnaire 2.

Afterward, Questionnaire 2 (Appendix B) is designed using the Degree of Belief (DoB) framework with three dimensions for each threat based on the concept of Failure Modes and Effects Analysis (FMEA): the likelihood of the threat, the consequence of the threat, and the probability of the threat going undetected. Through the analysis of the

Rule-based Bayesian Network (RBN) using GeNIe software, the results indicate that the most significant threat category is Malware, followed by Phishing, Human Factors, Theft of Credentials, Man in the middle attacks, and the use of outdated IT systems. In terms of threats, the top five significant ones are Accessing links from suspicious emails (Mal1), Connecting USB or removable media to a computer without a virus check (Mal3), Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it) (HF1), Downloading attached files from unknown emails (Mal2), and Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.) (Ph1).

Furthermore, a sensitivity analysis is employed to validate the proposed Bayesian Network (BN) model. The cases for both very high (VH) and very low (VL) overall risk aspects are presented. For the VH overall risk aspect, the top two critical threats influencing the overall risk are Ph1 and 'Downloading attached files from impersonation emails (e.g., bank, credit card company, insurance company, etc.) (Ph2),' which have the most significant impact on overall risk. Conversely, for the VL overall risk, the top two critical threats are Ph2 and Ph1. The results validate the proposal BN model with the achievement of the two Axioms, which are (1) An increase/decrease in the probabilities of each cyber threat should generate a relative increase/decrease in the risk. (2) Given the variation of the probability distributions of each cyber threat, its influence magnitude on the risk values should keep consistent.

The main contributions of this chapter are fourfold. First, this research aids to identify a list of maritime cyber threats. Based on their characteristics, it groups them into six categories, including ‘Phishing’, ‘Malware’, ‘Man in the middle attack’, ‘Theft of credential’, ‘Human factor’, and ‘Using outdated IT systems’ (see Table 3-8). This categorised structure is also validated by a number of maritime experts (see Table 4-7). Second, this research proposes a BN model for maritime cybersecurity risk analysis (see Figure 4-1). The proposed BN model is new and generic and hence can be further expanded to include more threats and/or categories (such as political risks, terrorism, piracy attacks, etc.). It thus provides a new direction for future research. Third, this

research assesses the criticality of the proposed cyber threats (see Table 4-10). Through the results of this research, maritime managers are now aware of which cyber threats and categories are relatively security critical and thus where they should focus their efforts especially given restricted budgets. For academia, the findings highlight the crucial maritime cyber threats for future research to conduct a more in-depth analysis of these threats.

In the meantime, a few limitations could be addressed in future research. First, the number of responses could have been higher. The response rate to questionnaires was around 40%; this is probably because the questionnaires (especially the second one) are complicated and not easy to be answered. Although the results are tested to be reliable and insightful, a higher number of responses could lead to new perspectives.
Second, although all respondents have some experience related to cybersecurity issues, one might argue that higher confidence should be placed on more experienced experts. Future research could weigh the expert opinion based on the level of familiarity with maritime cybersecurity and years of experience. On the other hand, one might argue that younger (and thus less experienced) domain experts might be more cybersecurity aware as younger groups are more familiar with modern IT systems. An interesting finding of analysis is that junior respondents have a higher mean value in most cyber threat estimates compared to that of senior experts. This can be a notable insight for seafarers' training and company managers should pay more attention to enhancing the cybersecurity awareness of more senior staff. Future research can also address the risk perception of different respondents' backgrounds (e.g., based on their position, department, education, work experience, etc.) through the use of statistics such as t-test or Analysis of Variance (ANOVA) models. The finding will provide further justification for the implementation of different control measures with regards to various stakeholder groups.

Furthermore, threats related to onboard systems are not always the same as those related to office computers; there are also differences in the network design and systems used in administration offices and those, say, in ports. Similarly, the

consequences of an attack on a small shipping company are not the same as those of a similar attack on a large company, an international organisation, or a governmental office. To address these differences, a more target- specific approach could be used. In this case, the assessed threats should be more carefully selected and should be more specific to the targeted systems and stakeholder groups.

This chapter's sensitivity analysis showcased only the very high and very low scenarios. Nevertheless, providing an overview of the entire spectrum, encompassing all parameters from Very High to Very Low, is available to obtain a more nuanced sensitivity analysis outcome. Subsequent studies aim to bolster the validity and reliability of results by conducting sensitivity analyses at various levels. This approach seeks to demonstrate the consistency of the relationship between risk exposure and risk management strategies across different discretisation methods (Bai et al., 2022).

Finally, this chapter mainly focuses on identifying and, more importantly, assessing the importance of cyber threats in the maritime industry. Several general measures are proposed to deal with cyber threats, but further research is required from the perspectives of the evaluation of measures to reduce the risk and select the most cost-effective ones for cybersecurity and resilience in the maritime industry.

5

ASSESSING THE EFFECTIVENESS OF CYBER RISK CONTROL MEASURES

5.1 Introduction

As discussed in the previous chapters, the industry needs to take steps to protect itself from cyber threats. Failure to address them can have devastating consequences in terms of human fatalities, loss of assets, and reputation. It can also lead to economic damages and environmental-related consequences. Given these increasing concerns about maritime cybersecurity, the shipping industry is urgently seeking measures to address cyber risk from both administrative and regulatory perspectives (e.g., the IMO) and operational perspectives (e.g., shipowners or operators).

In the light of the above, this chapter aims at analysing the effectiveness and efficiency of a set of cybersecurity mitigation measures currently being promoted in various guidelines or used in practice. In practice, selecting appropriate risk control measures (RCMs) is not an easy task as it involves balancing the potential benefits derived from their implementation against costs, effort, or disadvantages of their implementation. In order to identify the most cost-effective solutions, this chapter uses a Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) method because of its visibility and ease compared to other Multiple Criteria Decision Making (MCDM)

techniques. It evaluates and ranks the most widely used RCMs against six criteria, which are identified through a thorough state-of-the-art literature review.

It is anticipated that these measures will help prevent potential cybersecurity incidents and mitigate their adverse impacts. Having a set of preparedness and prevention measures in place to reduce security threats can enhance the resilience capability of companies. This assertion is supported by empirical studies that have demonstrated the significance of security management practices in bolstering the resilience of maritime companies (Yang and Hsu, 2018).

The work therefore makes new contributions on a) the development of a methodology to enable the effective evaluation of cybersecurity RCMs; b) the identification of all the essential criteria for supporting the evaluation; c) the collection of empirical data to realise the ranking of the currently established RCMs; and d) providing risk-informed policymaking for rational maritime cybersecurity assurance.

The rest of this chapter is organised as follows: Section 4.2 reviews and set a problem through the relevant literature and a set of criteria, along with identifies a list of cybersecurity risk mitigation measures to evaluate them. Section 4.3 describes the methodology, and Section 4.4 presents the results. Section 4.5 provides discussions and policy implications, and the conclusion and possible suggestions for future research are drawn in Section 4.6.

5.2 Problem Setting

To mitigate the consequences of cyberattacks, it is essential to address relevant risks. This involves identifying threats and vulnerabilities and developing protective and detection measures to reduce these risks. The goal is to minimise the likelihood of vulnerabilities being exploited and/or the severity of their impact. Our aim is to provide high-level recommendations, and as such, the Risk Control Measures (RCMs) is expressed in broad terms. To achieve this, the most commonly used RCMs (referred to

as 'alternatives' in the Multiple Criteria Decision-Making terminology) were identified through a literature review (see Section 5.2.1 for more details).

For information on the classical and fuzzy TOPSIS state-of-the-art, their applications, advantages, and main challenges, please refer to Behzadian et al. (2012) and Salih et al. (2017). TOPSIS has been used to rank decision alternatives according to defined criteria in various maritime problems such as the selection of the most suitable ballast water treatment systems (Karahalios, 2017), to determine the safety performance of flag states based on port state control inspections (Kara, 2022), to prioritise maritime cargo during the Covid-19 pandemic (Kontovas and Sooprayen, 2020) or even to measure the difference in development level of the marine shellfish industry in major producing countries (Peng et al., 2019).

In this study, a fuzzy TOPSIS approach is used; a comparison of the results with other methods are presented to validate the selected methodology. A comparison of fuzzy approaches is offered in Ceballos et al. (2017); there is much evidence that several approaches lead to similar, if not the same, ranks. This is an important result as methodology in this chapter utilises the fuzzy TOPSIS methodology in order to rank a number of alternatives in an attempt to provide useful managerial insights. In this sense, the robustness of the results can be ensured (as similar methods would arrive at the same results) and, therefore, so do recommendations.

To summarise, through a literature review, seven RCMs to reduce maritime cybersecurity risks and six criteria for assessing them have been identified and discussed in more detail in the following sections. Figure 5-1 illustrates the hierarchy structure and presents the relationship between the above identified criteria and the measures or strategies to be assessed.

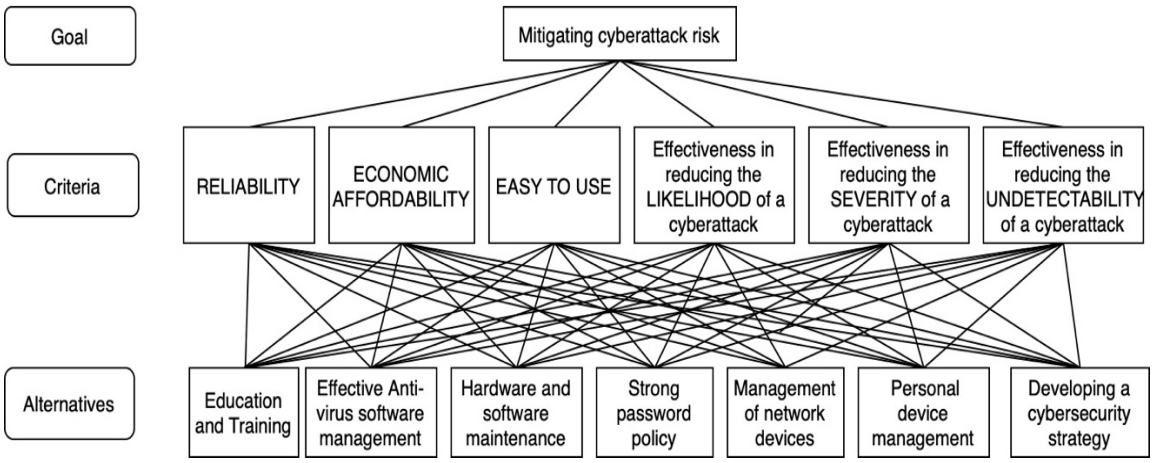


Figure 5-1: Hierarchy of maritime cybersecurity RCM evaluation

5.2.1 Mitigation Measures

Education and training

Education for new staff and regular training for all staff is essential. Education and training sea crew and staff is argued to be an effective method to enhance the maritime cybersecurity (Jones et al., 2016; Senarak, 2021; Corallo et al., 2022). These papers suggest that sea crews should be educated to deal with cyber incidents manually to protect the on-board systems and reduce damage to the equipment. Furthermore, Erstad et al. (2022) highlighted that the absence of policies, training, and regulatory standards is evident in how seafarers currently use vessel computer and control systems without due cybersecurity. Nevertheless, limited discussion exists on how companies can educate seafarers to effectively address existing threats (Karahalios, 2020; Canepa et al., 2021). Consequently, BIMCO (2018) has noted that the maritime industry lacks a cyber-awareness culture, potentially resulting in more vulnerabilities and a higher frequency of cyberattack incidents. To address this concern, the IMO has taken steps to enhance cybersecurity awareness. Shipping companies have been required to develop cybersecurity management systems since January 1, 2020, as outlined in IMO document MSC. 428 (98). Several classification societies offer relevant awareness programs, such as the Korean Register (KR), which provides a cybersecurity education program to train crew members on increasing their cybersecurity awareness, including the identification of cybersecurity threats.

Effective antivirus software management

The BIMCO (2018) report highlighted that the number of maritime cyber incidents had reached critical levels due to software maintenance and patching failures. They emphasised the importance of installing anti-virus programs on all work-related computers aboard vessels to reduce the risk of cyberattacks. Furthermore, their findings indicated that uninstalling anti-virus programs could lead to data loss, unauthorised access to information, network connectivity issues, and vulnerability to distributed denial-of-service (DDoS) attacks (Boyes and Isbell, 2017; Guanah, 2021).

Hardware and software maintenance

Updating on board security and safety systems should be an essential priority. That is the case for important Operation Technology (OT) systems such as Supervisory Control and Data Acquisition systems, Global Positioning Systems (GPS) and Distributed control systems (DCS). These kinds of systems have a long lifecycle and should be maintained and patched regularly; this is critical in mitigating cyber risk. However, sometimes, updates would not be received for any software or hardware that stops being supported by its software developer or producer (Guanah, 2021). To keep software updated to the latest version, a schedule of maintenance cycles should enable a key priority of software providers as well (Lagouvardou, 2018; Fischer-Hübner et al., 2021). Fitton at al. (2015) suggested that it is necessary to always update software systems to the latest versions in order to mitigate cyber risks. This is because through the development of advanced technology, many viruses and malicious programmes are also created simultaneously. The maritime industry must continuously update or even upgrade its IT systems, not only to address the threat of cyberattacks but also to maintain competitiveness (Svilicic et al., 2020).

Strong password policy

Mandating the use of complicated passwords and requiring users to change them regularly are widely recognised as a low-cost and easily implemented measure against cyber threats (National Cyber Security Centre, 2019). A poor password practice could cause unauthorised access and data breaches (IMO, 2018). The lack of password management, especially in the shipping industry, is exasperated by the fact that many

vessel systems are used by multiple crew members who all share passwords (Alcaide and Llave, 2020). Therefore, a strong password policy is recommended to deal with the risk of unauthorised access (Koola, 2018). Ensuring a strong password policy may involve mandating regular password updates and implementing multi-factor authentication wherever possible (BIMCO, 2018).

Personal device management

Recently, the use of Bring Your Own Device (BYOD) —refers to being allowed to use one's personally owned device, rather than a company provided device— such smartphones have been extended in the information and communication environment. Cyberattacks are also rapidly changing from traditional information and communication systems to infrastructure control systems, requiring structural changes in vulnerability analysis and evaluation methods (Dellios and Papanikas, 2014). Personal devices such as laptops, smartphones, and USB drives could be used to install malicious programmes into operation and information systems. Hardware vulnerabilities largely pertain to the reliability of the system and the data on it. For instance, Electronic Chart Display and Information System (ECDIS) can be updated via USB drives or the Internet; during this process, unauthorised USB drives may cause data loss or load malicious programs to OT systems (Pseftelis and Chondrokoukis, 2021). Therefore, effective management of personal devices can ensure that the crew's personal devices (e.g., smartphones and laptops) are unable to access sensitive systems such as navigation systems and other critical areas of the network.

Management of network devices

Most devices and systems do not operate in isolation; they communicate with each other, forming a network, and can also be accessed from the 'outside' world. This connectivity exposes them to various cyberattack threats, including network protocol attacks, network monitoring, and sniffing. To mitigate these threats, network configuration measures such as the use of proxy servers, encryption, firewalls, and Virtual Private Networks (VPN) are recommended. These measures help determine which systems should be attached to controlled or uncontrolled networks to prevent security risks through connected devices (Jang-Jaccard and Nepal, 2014; Boyes and Isbell,

2017). Network systems that should be placed on controlled networks include those used to provide suppliers with remote access to OT software and networks essential to the operation of a vessel. Misconfigured firewalls and proxy servers can lead to errors in network systems both onboard vessels and onshore (BIMCO, 2020).

Developing a cybersecurity strategy

Several guidelines recommend setting up cybersecurity strategies to protect assets from cyberattacks and to guide the actions should cybersecurity incidents happen. The IMO (2017a) has issued a document entitled "Guidelines on maritime cyber risk management" suggesting five functional steps that support effective cyber risk management: "Identify, Protect, Detect, Respond, Recover". BIMCO (BIMCO, 2016) also suggested a similar cyber risk management approach with the following steps: "Identify threats, Identify vulnerabilities, Assess risk exposure, Develop protections detection measures, Establish contingency plans, Respond to and recover from cybersecurity incidents".

5.2.2 Assessment Criteria

Having identified a number of RCMs to mitigate the cybersecurity risks, the next step is to identify a set of criteria that can be used to assess them. This is a common approach in dealing with MCDM problems; different alternatives (in this case the RCMs presented above in Section 4.2.1) are evaluated against a set of criteria to formulate a comparison of the alternatives. Criteria are selected through a literature review, and the chosen criteria, along with relevant literature supporting their use, are presented below.

Reliability

Reliability has been identified as an important factor in determining a cyber-risk strategy (Li and Kang, 2015). In the context of this work, reliability refers to the capability of these measures to perform as designed, even under specific conditions, and to their resilience in case of failure (Li and Kang, 2015).

Economic affordability

While the number of cybersecurity incidents has been rising, entities such as shipping companies and port authorities face financial constraints when addressing cybersecurity

risks. According to Hayes (2016) and Lee and Wogan (2018), the majority of companies allocate 1% to 2% of their overall budget to cybersecurity management. Consequently, it is crucial for companies to maximise the cost-effectiveness of their limited budgets. Affordable measures, in this context, are those that have low initial costs and are economical to operate over their lifetime.

Easy to use

Cybersecurity RCMs that are simple (for example in their design, use and implementation) are the ones that are preferred by the industry (BIMCO, 2020). Sea crew who only has a basic level of knowledge of cybersecurity might have difficulties to understand the concepts and mechanisms of much complicated cybersecurity and the relevant measures. Therefore, it is imperative to apply easy to use cybersecurity measures and strategies (Pseftelis and Chondrokoukis, 2021). This criterion refers to how straightforward and simple it is to use/implement the strategy.

Effectiveness in reducing the LIKELIHOOD of cyberattack

It is essential that the proposed measures can effectively reduce cybersecurity risks. The alternatives should therefore be assessed based on their effectiveness in terms of overall risk reduction. FMAE as a common method for risk assessment, presents a systematic approach based on three attributes: (a) the likelihood of failure, (b) the consequence of severity, and (c) the probability of the failure being undetected. FMEA has been wildly applied in the maritime sector (Yang et al., 2008; Chang et al., 2021). In this chapter, and following the concept of FMEA, the effectiveness of the defined alternatives was assessed through the three risk parameters. The likelihood part refers to how important the effectiveness in reducing the likelihood of being cyberattacked is in the selection of the best alternative i.e., mitigation measure to be introduced.

Effectiveness in reducing the SEVERITY of cyberattack

The second attribute is the effectiveness in reducing the severity of being cyberattacked; this refers to the effects/consequences following cyberattacks. Maritime systems, governing navigation and engine control, face cyber vulnerability, posing safety risks and environmental threats, such as oil spills (Akpan et al, 2022; Bueger and Liebetrau, 2023).

As a linchpin of the global economy, cyberattacks on the maritime industry disrupt operations, causing delays, and financial losses (Weaver et al, 2023). Beyond economic implications, the industry's role in transporting goods and military assets underscores its importance to national security (Afenyo and Caesar, 2023). Mitigating cyber risks in the maritime sector is essential for safeguarding lives, the environment, economic stability, national security, and data privacy in an increasingly digitised maritime landscape.

Effectiveness in reducing the UNDETECTABILITY of cyberattack

There are, for example, cases where cyberattacks can be detected before adverse consequences occur. Many threats though are not easily detected or, in practice, are in fact undetectable. The different measures/strategies are assessed for their effectiveness in reducing the undetectability of cyberattacks, which is equivalent to assessing their effectiveness in decreasing the probability/likelihood that the harm will occur. The detectability is indeed very important; even though many trustable architectures have been proposed (see Wang et al., 2022) many attacks, at least at their initial stages, are undetected. Some cyberattacks on the IT/OT systems may continuously shift nautical data in multiple messages to spoof several sensors simultaneously and remain undetected by possible integrity checks (Hemminghaus et al., 2021). Malicious programmes can stay undetected within the system specifications. According to Wimpenny et al. (2021), a security weakness was identified with the authentication scheme. In an extreme, but real, example of an undetected case, the cyberattack on the Danish Maritime Authority (DMA) which started in 2012 was only discovered in 2014. It has been found that a PDF (Portable Document Format) document was infected with a virus, which propagated from DMA to other government organisations (Park et al., 2019). In addition, some cybersecurity threats such as phishing or the man in the middle attack can indeed steal important data or information without being even noticed (Ashraf et al., 2022).

5.3 MCDM Methodology

As outlined above, the research addresses the issue of identifying effective cybersecurity RCMs. The various measures are assessed, and a rank is produced, facilitating the identification of the 'best' measures. This is important so that the industry directs its efforts towards the measures that stakeholders believe are the most important ones. The proposed fuzzy TOPSIS approach (following the classical approach as per Hwang and Yoon (1981)) is briefly described below to keep the work self-contained.

5.3.1 Classical TOPSIS

TOPSIS is a classical method, which ranks alternatives based on the concept that "the best alternative should have the shortest distance from the positive ideal solution (PIS) and the longest geometric distance from the negative ideal solution (NIS)" (Hwang and Yoon, 1981; Hwang et al., 1993). TOPSIS is one of the most well-established methods and has been applied in many fields due to being intuitive and easy to implement (Mardani et al., 2015). For a literature review of TOPSIS applications, please, see Behzadian et al. (2012).

5.3.2 Fuzzy Theory

Fuzzy models, for example using triangular fuzzy numbers, have been used very effectively in solving decision-making problems where the available information is imprecise. Some basic definitions of fuzzy sets and fuzzy arithmetic based on Dağdeviren et al. (2009) are provided below.

Definition 1. A fuzzy set $\tilde{A}$ in a universe of discourse X is characterised by a membership function $\mu_{\mathcal{A}}(x)$ that assigns a real number in the interval $[0; 1]$ to each element x. The value $\mu_{\tilde{A}}(x)$ is termed the grade of membership of x in $\tilde{A}$.

Definition 2. A triangular fuzzy number $\tilde{a}$ is defined by a triplet $\tilde{a} = (a_1, a_2, a_3)$ as shown in Figure 5-2.

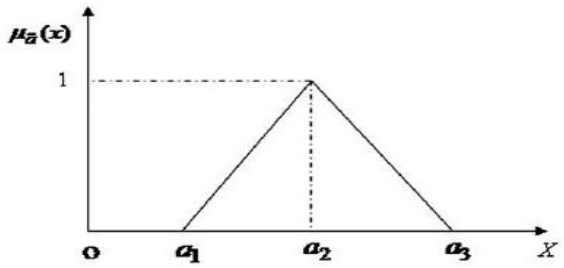


Figure 5-2: Triangular fuzzy number

The membership function is defined as follows:

$$\mu_{\tilde{a}}(x) = \begin{cases} 0, & x < a_1 \\ \dfrac{x - a_1}{a_2 - a_1}, & a_2 \geqslant x \geqslant a_1 \\ \dfrac{x - a_3}{a_2 - a_3}, & a_3 \geqslant x \geqslant a_2 \\ 0, & x > a_3 \end{cases}$$

where a_2 represents the value for which $\mu_{\tilde{a}}(a_2) = 1$, and a_1 and a_3 are the most extreme values on the left and on the right of the fuzzy number $\tilde{a}$, respectively with membership $\mu_{\tilde{a}}(a_1) = \mu_{\hat{a}}(a_3) = 0$; as per Figure 5-2.

Definition 3. Some main operations (such as addition, subtraction, multiplication and division etc.) of positive fuzzy numbers $\tilde{a} = (a_1, a_2, a_3)$ and $\tilde{b} = (b_1, b_2, b_3)$ can be expressed as follows:

$$\tilde{a} \oplus \tilde{b} = (a_1, a_2, a_3) \oplus (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3)$$
$$\tilde{a} \ominus \tilde{b} = (a_1, a_2, a_3) \ominus (b_1, b_2, b_3) = (a_1 - b_3, a_2 - b_2, a_3 - b_1)$$
$$\tilde{a} \otimes \tilde{b} = (a_1, a_2, a_3) \otimes (b_1, b_2, b_3) = (a_1 \cdot b_1, a_2 \cdot b_2, a_3 \cdot b_3)$$
$$\tilde{a} \oslash \tilde{b} = (a_1, a_2, a_3) \oslash (b_1, b_2, b_3) = \left(\frac{a_1}{b_3}, \frac{a_2}{b_2}, \frac{a_3}{b_1}\right)$$
$$k\tilde{a} = k(a_1, a_2, a_3).$$

Definition 4. Be two triangular fuzzy numbers $\tilde{a} = (a_1, a_2, a_3)$ and $\tilde{b} = (b_1, b_2, b_3)$ then the (Euclidean) distance between them is calculated by:

$$d(\tilde{a}, \tilde{b}) = \sqrt{\frac{1}{3}[(a_1 - b_1)^2 + (a_2 - b_2)^2 + (a_3 - b_3)^2]}$$

5.3.3 Fuzzy TOPSIS

In the classical TOPSIS approach, the performance ratings and the weights of the criteria are given as crisp values. In this chapter, the whole processes of fuzzy TOPSIS approach are adopted from Chen (2000). As first described in Chen (2000), which recognises that human judgement cannot be easily expressed by exact numbers and, therefore, a linguistic assessment for both the ratings and the weights of the criteria is used. The extension of the TOPSIS to a fuzzy environment is straightforward; the approach is very similar to that of the classical TOPSIS. The main difference is that fuzzy numbers are used instead of crisp numbers and fuzzy arithmetic is utilised. The methodology is illustrated in Figure 5-3.

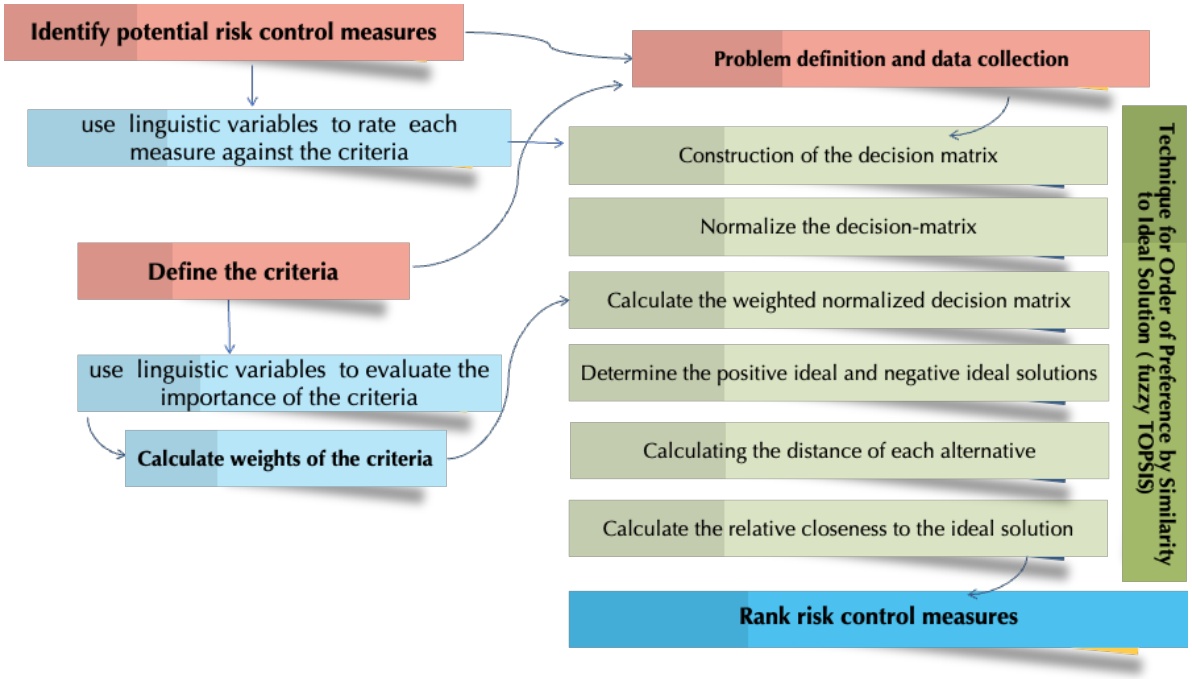


Figure 5-3: The Fuzzy TOPSIS methodology employed in Chapter 4

Step 1: Problem definition and data collection

In this step the problem is defined i.e., by identifying the alternatives and the criteria that will be used in assessing them; see Figure 5-1. This can be done through literature review and expert judgement; see Sections 5.2.1 and 5.2.2.

Then, it is needed to gather all the data that are necessary to solve the problem. As in most multi-criteria decision analysis methodologies, the inputs are a set of alternatives,

a set of criteria/parameters, the weights of each criterion (wj) and the rating (xij) of alternative Ai with respect to criterion Cj.

Aggregation of the importance of the criteria – weighting

The importance of each criterion/attribute can be obtained by different methods, for example by direct assignment or indirectly using pairwise comparisons; the latter is widely used in the AHP method. In this work, and in line with Chen (2000), a group of experts provides their opinion on the importance of each criterion using linguistic variables represented as triangular fuzzy numbers (See Table 5-1).

Table 5-1: Linguistic variables for the importance weight of each criterion

Linguistic Variable	Fuzzy number
Very low (VL)	(0, 0, 0.1)
Low (L)	(0, 0.1, 0.3)
Medium low (ML)	(0.1, 0.3, 0.5)
Medium (M)	(0.3, 0.5, 0.7)
Medium high (MH)	(0.5, 0.7, 0.9)
High (H)	(0.7, 0.9, 1)
Very high (VH)	(0.9, 1, 1)

Assuming a group of K decision makers (or experts), then the importance of the criteria can be calculated as the simple average:

$$\tilde{w_j} = \frac{1}{K}\left[\tilde{w_j^1}\ (+)\ \tilde{w}_j^2 (+) \ldots (+) \tilde{w_j^K}\ \right]$$

where $\tilde{w}_j^K$ is the importance weight (represented as a fuzzy triangular number) of the K-th decision-maker.

Aggregation of the ratings

The experts provide their ratings using the linguistic terms presented in Table 5-2.

Table 5-2: Linguistic variables for the ratings

Linguistic Variable	Fuzzy number
Very Poor (VP)	(0, 0, 1)
Poor (P)	(0, 1, 3)
Medium Poor (MP)	(1, 3, 5)
Fair (F)	(3, 5, 7)
Medium Good (MG)	(5, 7, 9)
Good (G)	(7, 9, 10)
Very Good (VG)	(9, 10, 10)

Assuming that the decision group has K persons, the rating of alternatives with respect to each criterion can be calculated as follows:

$$\tilde{x}_{ij} = \frac{1}{K}\left[\tilde{x}_{ij}^{1}\,(+)\,\tilde{x}_{ij}^{2} + \cdots + \tilde{x}_{ij}^{K}\right]$$

where $\tilde{x}_{ij}^{k}$ is the rating of the kth decision maker (represented as a fuzzy triangular number) for alternative A_i with respect to criterion C_j.

Step 2: Construction of the decision matrix

The fuzzy multicriteria group decision-making problem can then be expressed in matrix format as follows:

$$\widetilde{D} = \begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \dots & C_n \end{array} \\ \begin{bmatrix} \tilde{x}_{11} & \tilde{x}_{12} & \dots & \tilde{x}_{1n} \\ \tilde{x}_{21} & \tilde{x}_{22} & \dots & \tilde{x}_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \tilde{x}_{m1} & \tilde{x}_{m2} & \vdots & \tilde{x}_{mn} \end{bmatrix} \end{array}, i = 1,2,\dots,m; \quad j = 1,2,\dots,n$$

where $A_1, A_2, \dots, A_m$ are alternatives, $C_1, C_2, \dots, C_n$ are criteria, $\tilde{x}_{ij}$ are fuzzy numbers that indicate the rating of the alternative A_i with respect to criterion C_j.

Step 3: Normalisation of the decision matrix

The data are usually normalised to eliminate deviations with different measurement units and scales. Normalisation is an operation to make these scores conform to, or reduced to, a norm i.e., the normalised values will be positive values between 0 and 1.

The linear scale transformation is used in this work to transform the various criteria scales into a comparable one.

The normalised fuzzy decision matrix denoted by $\tilde{R}$ can therefore be calculated as follows:

$$\tilde{\boldsymbol{R}} = \left[\tilde{r}_{ij}\right]_{m\times n}$$

where B and C are the set of benefit criteria and cost criteria, respectively, and

$$\begin{aligned}
\tilde{r}_{ij} &= \left(\frac{a_{ij}}{c_j^*}, \frac{b_{ij}}{c_j^*}, \frac{c_{ij}}{c_j^*}\right),\ j \in B \\
\tilde{r}_{ij} &= \left(\frac{a_j^-}{c_{ij}}, \frac{a_j^-}{b_{ij}}, \frac{a_j^-}{a_{ij}}\right),\ j \in C \\
c_j^* &= \max_i c_{ij} \ \text{ if } j \in B \\
a_j^- &= \min_i a_{ij} \ \text{ if } j \in C.
\end{aligned}$$

Step 4: Construction of the weighted normalised decision matrix

The weighted normalised fuzzy-decision matrix $\tilde{P} = \left[\tilde{p}_{ij}\right]_{\text{mxn}}$ with $i = 1, \ldots, m$, and $j = 1, \ldots, n$ is then calculated by multiplying the normalised decision matrix by its associated (fuzzy) weights. The weighted fuzzy normalised value $\tilde{p}_{ij}$ is calculated as: $\tilde{p}_{ij} = w_i \tilde{x}_{ij}$ with $i = 1, \ldots, m$, and $j = 1, \ldots, n$.

Step 5: Calculating the positive and negative ideal solution

The PIS A^+(benefits) and NIS A^-(costs) are identified as follows:

$$A^+ = (\tilde{p}_1^+, \tilde{p}_2^+, \ldots, \tilde{p}_m^+)$$

$$A^- = (\tilde{p}_1^-, \tilde{p}_2^-, \ldots, \tilde{p}_m^-)$$

where $\tilde{p}_j^+ = (1,1,1)$ and $\tilde{p}_j^- = (0,0,0), j = 1,2, \ldots, n.$

Step 6: Calculating the distance of each alternative

In this step the distance of each alternative A_i from the PIS $A^+$and the NIS A^-, respectively, are calculated as follows:

$$d_i^+ = \sum_{j=1}^{n} d\left(\tilde{p}_{ij}, \tilde{p}_j^+\right), \text{ with } i = 1, \ldots, m \ \text{ and}$$

$$d_i^- = \sum_{j=1}^{n} d\left(\tilde{p}_{ij}, \tilde{p}_j^-\right), \text{ with } i = 1, \ldots, m$$

where the distance $d\left(\tilde{p}_{ij}, \tilde{p}_j^+\right)$ is defined in *Definition 4* in previous Fuzzy theory part.

Step 7: Calculating the relative closeness to the ideal solution and scoring the alternatives

Calculate the relative closeness ξ_i for each alternative A_i with respect to PIS as given by:

$$\xi_i = \frac{d_i^-}{d_i^+ + d_i^-}$$

The alternatives are ranked according to their relative closeness. The best alternatives are those that have higher value ξ_i and therefore should be chosen because they are closer to the PIS.

5.4 Data Analysis

5.4.1 Questionnaire Design

Data have been obtained using an online questionnaire with three sections.

The first section asks the respondents to provide information regarding their work experience and type of the company they are working in.

In the second section of the questionnaire, the experts were asked to provide their opinions on the importance of each criterion for the selection of the cybersecurity RCMs to address cyberattacks; see Figure 5-4. In the final section, the respondents' ratings were elicited regarding the seven identified measures, using seven linguistics terms (from very poor to very good); see for example Figure 5-5 that presents the question related to the rating of the alternatives with respect to their effectiveness in reducing the 'Likelihood' of cyberattacks, and full questionnaire is presented in Appendix C.

The sampling methods are as described in Section 3.3. Non-probability sampling methods were utilised for all our questionnaires, starting with a purposeful sampling, i.e., selecting participants based on their expertise or knowledge in the specific field, but who are also easy to reach and willing to participate. In order to a high number of responses, experts were asked to recommend other experts they know, employing a technique known as 'snowball sampling.'

How important are the criteria below for the selection of the best alternative (strategy) to address the risk of cyber-attacks? (PLEASE select only one value per row/criterion) *

Mark only one oval per row.

	Very low	Low	Medium low	Medium	Medium high	High	Very high
RELIABILITY	◯	◯	◯	◯	◯	◯	◯
ECONOMIC AFFORDABILITY	◯	◯	◯	◯	◯	◯	◯
EASY TO USE	◯	◯	◯	◯	◯	◯	◯
Effectiveness in reducing the LIKELIHOOD of a cyberattack	◯	◯	◯	◯	◯	◯	◯
Effectiveness in reducing the SEVERITY of a cyberattack	◯	◯	◯	◯	◯	◯	◯
Effectiveness in reducing the UNDETECTABILITY of a cyberattack	◯	◯	◯	◯	◯	◯	◯

Figure 5-4: Questionnaire: Importance of criteria

Rate the alternatives with respect to 'Effectiveness in Reducing the LIKELIHOOD of Cyberattack' (limited to one response per row). Scale from Very poor (e.g. Very low effect in reducing the likelihood) to Very good (e.g. very good/ effective in reducing the likelihood) *

Mark only one oval per row.

	Very poor	Poor	Medium poor	Fair	Medium good	Good	Very good
Education and Training	◯	◯	◯	◯	◯	◯	◯
Effective Anti-virus software management	◯	◯	◯	◯	◯	◯	◯
Hardware and software maintenance	◯	◯	◯	◯	◯	◯	◯
Strong password policy	◯	◯	◯	◯	◯	◯	◯
Management of network devices	◯	◯	◯	◯	◯	◯	◯
Personal device management	◯	◯	◯	◯	◯	◯	◯
Developing a cybersecurity strategy	◯	◯	◯	◯	◯	◯	◯

Figure 5-5: Questionnaire: Rating of alternatives

5.4.2 Profile of the Responders

A total of 105 responses have been received; of which 100 were used in analysis. Five responses were unsuitable; as they provided for example uniform answers i.e., they provided the same rating for all alternatives, or others provided scores that were extreme compared to the average values.

For validation purposes, the same analysis has been conducted without removing the outliers, and the same ranks have been obtained. Table 5-3 presents their profiles, noting that this info has not been disclosed by everyone. Over 50% of them are from shipping companies or ship operators, and 70% of them have more than 5 years of experience working in the maritime industry.

Table 5-3: Respondents' background

Organisation	Ship owner/operator	42
	Port operator	10
	Regulator	11
	Academia	12
	Other	25
Work experience	Less than 5 years	19
	6-10 years	19
	11-15 years	13
	More than 15 years	37

5.4.3 Results of Analysis

The weights are presented as fuzzy triangular numbers; their crisp values using the so-called graded mean integration are also presented. Based on the responders' opinion the most important criteria in the selection of the most appropriate measures are 'reliability', followed by the FMEA-inspired 'effectiveness in reducing the likelihood' and 'effectiveness in reducing the severity' respectively. The result of weight of criteria is illustrated in Table 5-4.

Table 5-4: Weight of criteria

	RELIABILITY	ECONOMIC AFFORDABILITY	EASE TO USE	Reducing LIKELIHOOD	Reducing SEVERITY	Reducing DETECTABILITY
Fuzzy Weights	(0.77,0.91,0.96)	(0.52,0.69,0.82)	(0.57,0.74,0.88)	(0.71,0.87,0.95)	(0.72,0.87,0.95)	(0.67,0.83,0.93)
Crisp values	0.1843	0.1405	0.1519	0.1769	0.1771	0.1693

5.4.4 Rank of Alternatives

The resulting decision matrix is shown in Table 5-5, and weighted normalised decision matrix is shown in Table 5-6. This decision matrix and the fuzzy weights are the main inputs to the fuzzy TOPSIS methodology presented in Section 4.3.

Table 5-5: Decision Matrix

	RELIABILITY	ECONOMIC AFFORDABILITY	EASE TO USE	Reducing LIKELIHOOD	Reducing SEVERITY	Reducing DETECTABILITY
A1	(6.16,7.84,8.98)	(5.49,7.21,8.50)	(6.13,7.77,8.84)	(5.88,7.55,8.67)	(6.01,7.69,8.83)	(5.61,7.32,8.54)
A2	(7.21,8.74,9.52)	(5.92,7.68,8.87)	(6.08,7.81,8.98)	(7.21,8.74,9.52)	(6.91,8.49,9.35)	(6.95,8.50,9.37)
A3	(6.72,8.44,9.47)	(5.48,7.31,8.68)	(5.19,7.03,8.49)	(6.68,8.41,9.47)	(6.70,8.40,9.42)	(6.40,8.17,9.30)
A4	(6.63,8.29,9.28)	(6.27,7.95,9.03)	(6.07,7.81,9.01)	(6.61,8.25,9.20)	(6.22,7.93,9.05)	(5.94,7.65,8.80)
A5	(6.51,8.21,9.27)	(6.07,7.82,9.01)	(5.57,7.42,8.75)	(6.56,8.30,9.39)	(6.36,8.11,9.23)	(6.48,8.22,9.29)
A6	(6.42,8.19,9.34)	(5.97,7.69,8.86)	(5.70,7.47,8.72)	(6.28,8.04,9.21)	(5.95,7.66,8.88)	(5.76,7.51,8.76)
A7	(6.62,8.27,9.25)	(5.75,7.47,8.69)	(5.75,7.49,8.77)	(6.54,8.21,9.22)	(6.65,8.28,9.24)	(6.58,8.24,9.24)

Table 5-6: Weighted normalised decision matrix

	RELIABILITY	ECONOMIC AFFORDABILITY	EASE TO USE	LIKELIHOOD	SEVERITY	DETECTABILITY
A1	(0.50,0.75,0.91)	(0.31,0.55,0.78)	(0.39,0.64,0.86)	(0.44,0.69,0.87)	(0.46,0.71,0.89)	(0.40,0.65,0.85)
A2	(0.58,0.83,0.96)	(0.34,0.58,0.81)	(0.38,0.65,0.87)	(0.54,0.80,0.95)	(0.53,0.79,0.94)	(0.49,0.76,0.93)
A3	(0.54,0.81,0.96)	(0.31,0.56,0.79)	(0.33,0.58,0.83)	(0.50,0.77,0.95)	(0.51,0.78,0.95)	(0.45,0.73,0.92)
A4	(0.54,0.79,0.94)	(0.36,0.61,0.82)	(0.38,0.65,0.88)	(0.50,0.75,0.92)	(0.47,0.73,0.91)	(0.42,0.68,0.87)
A5	(0.53,0.78,0.94)	(0.35,0.60,0.82)	(0.35,0.61,0.85)	(0.49,0.76,0.94)	(0.49,0.75,0.93)	(0.46,0.73,0.92)
A6	(0.52,0.78,0.94)	(0.34,0.59,0.81)	(0.36,0.62,0.85)	(0.47,0.74,0.92)	(0.45,0.71,0.90)	(0.41,0.67,0.87)
A7	(0.54,0.79,0.93)	(0.33,0.57,0.79)	(0.36,0.62,0.85)	(0.49,0.75,0.92)	(0.51,0.77,0.93)	(0.47,0.73,0.92)

Finally, the relative closeness to the ideal solutions has been calculated and alternatives were ranked based on this relative closeness value; see Table 5-7.

Table 5-7: Relative closeness to the ideal solutions and score of the alternatives

	A1	**A2**	**A3**	**A4**	**A5**	**A6**	**A7**
Distance from PIS	2.465	2.144	2.307	2.301	2.293	2.394	2.286
Distance from NIS	3.948	4.296	4.161	4.135	4.168	4.051	4.152
Relative closeness	0.616	0.667	0.643	0.642	0.645	0.629	0.645
Rank	7	**1**	4	5	**2**	6	**3**

Legend: A1 Education and training; A2 Effective Anti-virus software management; A3 Hardware and software maintenance; A4 Strong password policy; A5 Personal device management; A6 Management of network devices; A7 Developing a cybersecurity strategy.

Based on the above results the experts believe that the best approach (alternative/strategy) to mitigate the risk of cyberattacks is 'Effective Anti-virus software management' (A2), followed by 'Management of network devices' (A5) and 'Developing a cybersecurity strategy' (A7).

Note that the results of all MCDM methods (including this one) are sensitive to the weights used and the methodology used. In the classical approach a sensitivity analysis is usually presented; this is straightforward in the classical TOPSIS, where weights can slightly be changed to investigate the impact of changes in the final rankings. In this case, and in line with similar studies, see for example Yan et al. (2017) and Emovon and Aibuedefe (2020), a validation is performed by comparing this study results with those obtained using similar methods such as Fuzzy VIKOR (VIseKriterijumska Optimizacija I Kompromisno Resenje) and Fuzzy Weighted Aggregated Sum Product Assessment (Fuzzy WASPAS) is presented in detail in Table 5-8. As it can be seen, all methods agree in that A2 and A5 are the top measures to address cybersecurity risks. Possible limitations of this approach are discussed in conclusion part, but based on the above validation process it would be considered the results to be robust.

Table 5-8: Rank of measures produced by different methods

Alternatives	**TOPSIS** (Linear normalisation)	**MOORA**	**TOPSIS** (Vector normalisation)	**VIKOR** (v=0.5)	**WASPAS** (lambda=0.5)
A1	7	7	7	7	7
A2	1	1	1	1	1
A3	4	4	3	4	3
A4	5	5	5	5	5
A5	2	2	2	3	2
A6	6	6	6	6	6
A7	3	3	4	2	4

5.4.5 Discussion and Policy Implications

To begin with, it comes as no surprise that the stakeholders feel that the third most important measure to control the relevant risks is the development of a cyber-security strategy. BIMCO guidelines (BIMCO, 2020) were indeed introduced to "assist in the development of a proper cyber risk management strategy in accordance with relevant regulations and best practises on board a ship with a focus on work processes, equipment, training, incident response and recovery management." The need for a risk-based approach to managing risk is here expected; and indeed, many of the relevant studies, both academic and those in the 'grey literature', are in this area. Not to forget that there is an expectation of stakeholders to comply with the relevant regulations. In fact, the IMO Resolution MSC.428 (98) (IMO,2017b), requires ship owners and managers to assess cyber risk and implement relevant measures across all functions of their safety management system i.e., as part of the International Safety Management Code (ISM), until the first Document of Compliance (DOC) after 1 January 2021. In addition, it should be also mentioned that the IMO released the 'Guidelines on Maritime Cyber Risk Management' (see IMO,2017a) in July 2017. Both documents though, leave much of the interpretation to the shipping companies and from the literature survey, it is evident that there are still many uncertainties on how to handle the requirements.

Nevertheless, the results are clear; more must be done to make software and hardware systems more secure. Some measures are effective, easy to be implemented and not expensive: 'use an anti-virus', 'patch your systems', 'apply the latest software updates'. As mentioned in Section 5.2 a number of incidents were a result of the failure of software maintenance and patching of systems. There are actually many systems (software) vulnerabilities that are discovered by attackers even before the vendors are aware of them, these are known as 'zero-day vulnerabilities. Not much can be done about these attacks through software updates and patches but then perhaps a good approach is to better control the network devices and prevent unauthorised access from systems outside the network, for example using firewalls. A firewall is a network security device that monitors, and filters incoming (and also outgoing) network traffic and it can act as a barrier between the internal network and the 'outside world'. BIMCO guidelines indeed emphasise the importance of proper configuration of network devices such as firewalls, routers, and switches.

Meanwhile, anti-virus and anti-malware software packages are inexpensive solutions that detect viruses and malware and quarantine them so that they cannot cause any damage. Humans do not necessarily, even if trained, pay much attention when downloading software or files from unfamiliar or unreliable sources. Email viruses are also becoming increasingly popular; malicious code is distributed in email messages and when activated it can infect the devices. Therefore, while email attachments are deemed to be a popular and indeed convenient way to send and share files, they are also a very common source of viruses. Anti-virus software is, therefore, very important in preventing downloading and executing malicious code. Nowadays, anti-virus solutions often offer 'total protection' such as virus and malware protection, including also extra features like anti-phishing, virtual private networks (VPN) solutions and firewalls. In this sense, it comes to no surprise that based on the stakeholder's opinion this is the most effective solution to deal with cybersecurity risks.

Based on the above analysis, the following recommendations would be proposed to be considered by the maritime industry and the regulators. First, the industry should

prioritise investment in hardware and software as they can effectively and efficiently reduce the likelihood and the consequences of the equipment being cyberattacked. For example, although the 'Bring Your Own Device (BYOD)' policy has several significant advantages (e.g., cost savings for companies, reduced needs for IT training, etc.), these personal devices are easier to attack compared to company managed devices. Companies could implement several strategies to enhance cybersecurity, some of them are quite straightforward to implement.

Additionally, it is suggested purchasing and offering employees (also for their personal devices) a comprehensive anti-virus software. This is the most effective way to prevent malicious cyber risks from outside of the company, as well as the data breach from inside of the company. In addition, implementing personal device management (e.g., restricting the individual's devices to access the company's sensitive data) and developing a cybersecurity strategy (e.g., providing a guideline for sea crews and staff to easy to follow to reduce the likelihood of being cyberattack and to mitigate the impacts once being cyberattacked) are suggested. By implementing the above, companies can enjoy the advantages of BYOD, but also mitigate the cyber risks. At the same time, although implementing a strong password policy ranks fifth in this research, it cannot be denied that it is still a very effective and affordable way to address cybersecurity risks. Meanwhile, IMO Member-States should also urge the maritime industry to more strictly implement the 'Guidelines on Maritime Cyber Risk Management' proposed by the IMO to prevent and mitigate the impact of cyber risks on the maritime industry. Relevant inspections could take place by the Port State Control (PSC).

Although 'education and training' was ranked at the bottom in this research, without doubt it is very much important. A possible explanation is that the responders feel that this is covered by mandatory training which staff currently receives as part also of the relevant legal requirements and guidelines (see Sections 2.4 – 2.7). In any case, the maritime industry should keep educating and training staff and crews in order to better understand the importance of cybersecurity and to enhance their cybersecurity

awareness. The maritime industry could collaborate with higher education providers and/or maritime related associations, who help to educate and train crews and staff for the industry. The government could also recommend cybersecurity training, as well as offer recognised certificates to encourage more sea crews and shore-based staff to take the training (Kanwal et al., 2022).

5.5 Conclusions

In Chapter 4, a comprehensive approach to risk management necessitates not only assessing the significance of risk factors but also evaluating the significance of the Risk Control Measures (RCMs) designed to address these risk factors. Through an extensive review of the literature, this study has identified seven distinct RCMs relevant to the realm of maritime cybersecurity. These include 'Education and Training,' 'Effective Anti-Virus Software Management,' 'Hardware and Software Maintenance,' 'Strong Password Policy,' 'Management of Network Devices,' 'Personal Device Management,' and 'Developing a Cybersecurity Strategy'. To effectively prioritise these seven RCMs, a set of six criteria has been established. These criteria encompass attributes such as 'Reliability,' 'Economic Affordability,' 'Ease of Use,' 'Effectiveness in Reducing the Likelihood of a Cyberattack,' 'Effectiveness in Reducing the Severity of a Cyberattack,' and 'Effectiveness in Reducing the Undetectability of a cyberattack.

For gathering expert opinions regarding the significance of these RCMs, a questionnaire (Questionnaire 3, provided in Appendix C) has been meticulously designed utilising a seven-point Likert scale. The survey process yielded a total of 105 responses, with 5 responses deemed incomplete and hence excluded, resulting in a pool of 100 valid responses. Through the application of fuzzy Technique for Order Preference by Similarity to Ideal Solution (fuzzy TOPSIS) analysis, the findings of this study unveil that the most efficacious approach or alternative for mitigating the risk of cyberattacks is identified as 'Effective Antivirus software management' (A2), closely trailed by 'Management of network devices' (A5) and 'Developing a cybersecurity strategy' (A7).

In conclusion, there are several policy implications to consider. The maritime industry should prioritise investments in both hardware and software to reduce the likelihood and consequences of cyberattacks on its equipment. While the 'Bring Your Own Device (BYOD)' policy offers advantages like cost savings, it's essential to acknowledge that personal devices are often more vulnerable to cyberattacks than company-managed devices. Providing comprehensive anti-virus software to employees, even those using personal devices, is a simple yet effective cybersecurity measure. This proactive approach helps prevent cyber risks from external and internal sources, including data breaches. Additionally, it is advisable to restrict personal device access to sensitive data and establish clear cybersecurity guidelines for sea crews and staff to strike a balance between BYOD benefits and effective cyber risk mitigation. Despite lower priority in the research, ongoing education and training remain crucial for enhancing cybersecurity awareness within the maritime industry. This ensures that staff and crews are well-prepared to mitigate cyber threats effectively.

5.5.1 Limitations and Future Work

Methodology-wise, a number of possible extensions could be investigated; these are mainly related to the normalisation step and the distance measures used in the TOPSIS approach. Normalisation (see Step 3 of the process) is a fundamental step in all MCDM methods; using different methods (i.e., linear, logarithmic, Markovic, Tzeng and Huang method) and comparing the results could be a suggestion for future research. In addition, the final rank depends on the distance of each alternative from the PIS and NIS; the selected distance metric is therefore of paramount importance. The classical approach for group fuzzy TOPSIS (Chen, 2000) calculates the Euclidean distances; other approaches (such as the Manhattan or Tchebycheff distance) could be investigated; see Ploskas and Papathanasiou (2019) for the alternative approaches.

The refinement of the TOPSIS hierarchical model would be needed for further research. While the present study implemented a straightforward hierarchical model, future investigations will be required to delve deeper by incorporating more specialised sub-

criteria for alternatives. For instance, focusing on technology aspects, human factors, and process considerations will be intensified (DNV, 2023). The alternatives in this research would categorise human related (ex. education and training), technology related (ex. hardware and software maintain) and process related (ex. developing a cybersecurity strategy). The aim is to unravel nuanced options for cybersecurity risk control within these dimensions. This strategic expansion beyond the simplistic model is anticipated to yield comprehensive insights. By incorporating specific criteria such as technical intricacies, human-centric elements, and policy nuances, the research seeks to augment the granularity of cybersecurity risk control options. This evolution in methodology is poised to enhance the depth and precision of the analysis, providing a more nuanced understanding of the multifaceted landscape of cybersecurity risk management.

Sensitivity analysis could also be performed to test the impact of slight variations of the inputs to the final rank; for example, the impact of different weights. Performing a sensitivity analysis in a fuzzy environment is rather challenging given that the weights are fuzzy and not crisp numbers. Instead, to validate the findings and the use of the selected method, we used the same input data in various established MCDM methods such as Fuzzy VIKOR, Fuzzy WASPAS and Fuzzy Multi-Objective Optimisation by Ratio Analysis (MOORA). It is out of the scope of this research to discuss these methods (see Ceballos, 2017) for a comparison of these approaches. However, as it can be seen in Table 5-8, all the methods produced similar ranks for our input data. This is an interesting result, which shows that our results are robust. In practise this means that using other methods would indeed render similar results and our managerial/policy implications would, therefore, still be valid.

The critical areas for future investigation, include the various criteria to be utilised and, most importantly, the measures to be assessed. In this study the RCMs are expressed in broad terms in order to stimulate a widespread application as well as to address the uncertainty in data on the specific RCMs. There is, however, a need for more application-specific control measures, perhaps also identifying the prevention and recovery options

through a more systematic approach, for example through the use of bowtie analysis, Hazard and Operability Analysis (HAZOP), etc. In addition, the RCMs can focus on specific ship types and ship segments or focus in particular sectors of the maritime industry. According to Tonn et al. (2019), very few studies focus specifically on specifically on cyber risk in the transportation infrastructure industry; maritime ports are very vulnerable and could be the focus of dedicated studies using our proposed methodology.

Another interesting area would be also to compare the findings i.e., the ranks for different stakeholders in order to identify differences in the perspectives of, say, the seafarers and ship operators or policymakers, or between experts coming from different countries, or different age groups (assuming here that younger responders could be more familiar with modern information technologies). This will help stimulate the development the compromising policies that can be best accepted by all stakeholders and hence easier for their implementation.

In final, this study contributes to the advancement of cybersecurity research by proposing a new methodology. This methodology is designed to effectively evaluate cybersecurity Risk Control Measures (RCMs) through the application of fuzzy TOPSIS, supported by the collection of empirical data. The primary objectives include ranking currently established RCMs and identifying essential evaluation criteria. Ultimately, the research provides a foundation for risk-informed policymaking in the field of maritime cybersecurity assurance.

6

CYBERSECURITY RISK ASSESSMENT USING BOWTIE DIAGRAMS

6.1 Introduction of Bowtie Analysis

The Bowtie analysis was developed during a lecture on hazard analysis at The University of Queensland, Australia, in 1979, as part of the Imperial Chemical Industries course. In the early 1980s, Royal Dutch Shell became the first petrochemical company to apply bowtie analysis to its business practices (Center for Chemical Process Safety, 2018). Since then, the method has been widely used in other high-risk industrial fields, including oil and gas, chemical, mining, aviation, maritime, public health services, and processing sectors, as a qualitative Process Safety Management (PSM) method for proactive and reactive safety incident reviews (Aust and Pons 2020; Progoulakis et al. 2021).

The bowtie analysis is a risk management process that visualises a set of risk scenarios, from threats to consequences (Ferdous et al., 2013). The visualisation makes it easier to identify controls to minimise the likelihood of threats resulting in undesirable events and, on the recovery side, to reduce the severity of consequences if such events occur (Hurst and Lewis, 2005).

This chapter employs bowtie analysis to identify risk control barriers that can effectively mitigate and reduce the impact of cyberattacks in advance in the maritime sector. Additionally, previous Chapters 3 and 4 are scrutinised with greater academic rigour; however, this chapter serves a practical purpose, aiming to provide straightforward examples that industrial stakeholders can readily understand.

6.2 Bowtie Analysis Concept

The widely used industry Risk Management standard ISO 31010 (as discussed in Section 2.3.1) describes the bowtie analysis as a 'diagrammatic way of describing the pathways from sources of risk to outcomes and of reviewing controls.' It presents this methodology as a tool for describing, analysing, and evaluating risk and risk control measures. Bowtie analysis combines elements of fault tree analysis (FTA), event tree analysis (ETA), and barrier analysis (BA) (Tang et al., 2017). Hazards are systematically represented by describing their relationship to undesirable events, their causes, and their consequences (Akyuz et al., 2020).

Bowtie analysis combines fault tree analysis (FTA), event tree analysis (ETA), and barrier analysis (BA) (Tang et al., 2017)., and hazards are represented in systematic ways by describing their relationship to undesirable events, their causes, and their consequences (Akyuz et al., 2020). The risk sources and prevention barriers on the left side of the top events can be represented by FTA, but the detection and response barriers on the right side of the top events can be represented by ETA in bowtie analysis (de Ruijter and Guldenmund, 2016). Figure 6-1 presents of the generic concept of bowtie.

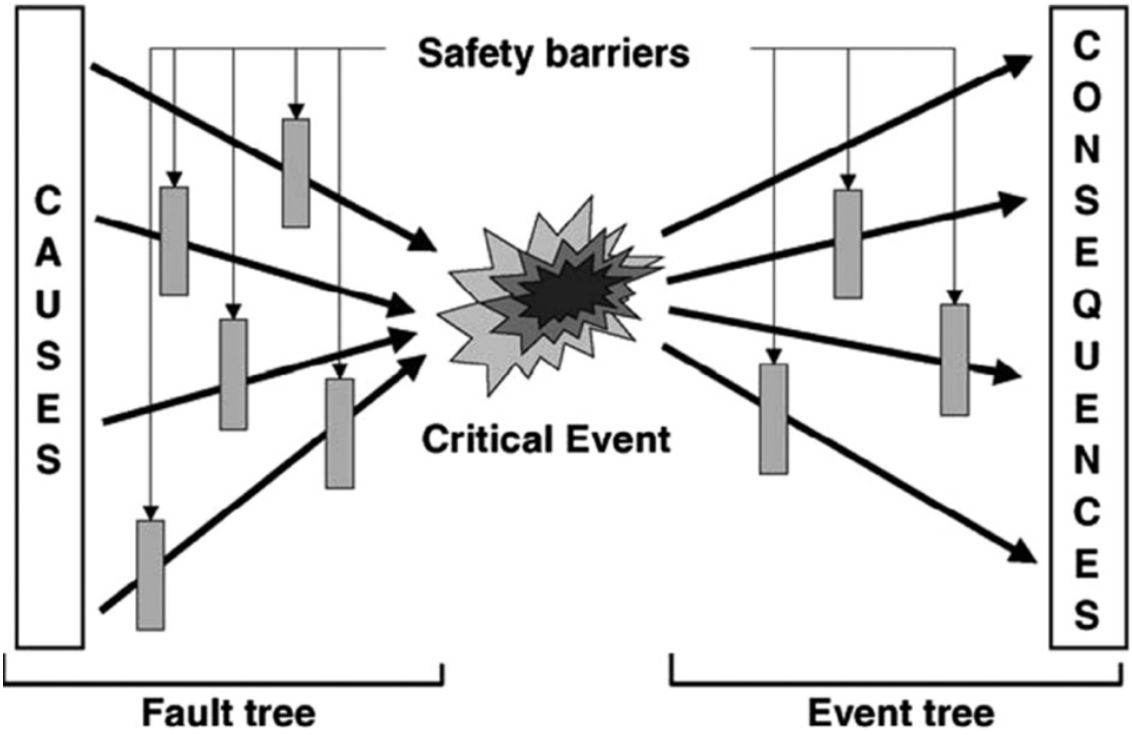


Figure 6-1: Generic concept of a bowtie - Source: de Ruijter and Guldenmund (2016)

6.2.1 Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA) is a graphic model used to illustrate various combinations of equipment defects and human errors that lead to failures in major systems. FTA employs deductive techniques, focusing on specific accidents or major system failures through the use of AND and OR gates. The AND gate signifies that all events related to a specific event occur simultaneously, while the OR gate indicates that an event is underway, involving the deployment of other related events (Voicu et al., 2018). The concept of FTA is depicted in Figure 6-2. FTA offers the advantage of visually representing complex relationships between failure paths and combinations of outcomes. Its structured and logical approach enables quantitative analysis of all potential root causes (Aust and Pons, 2019). Additionally, FTA can be used for both predicting future failures and diagnosing past failures. However, FTA has limitations, including challenges in quantifying probabilities, potential inaccuracies when data is scarce or unavailable, uncertainty in covering all failure modes and accounting for partial failures, as well as

accounting for external environmental effects and human behavioural effects (Fouladvand et al., 2010).

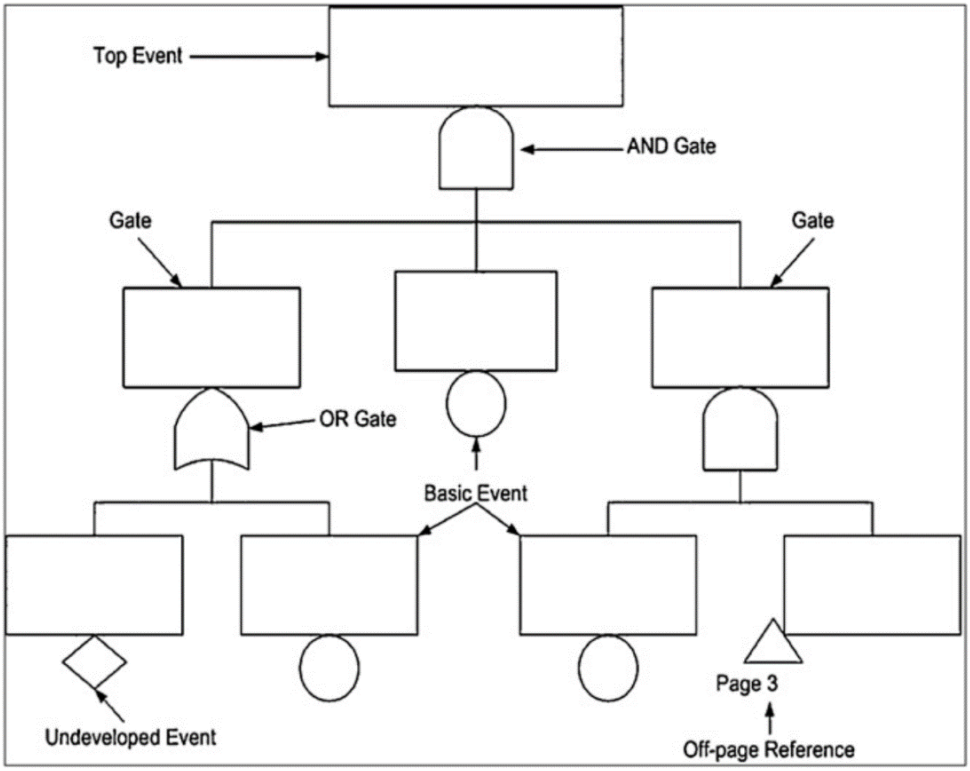


Figure 6-2: Example of the FTA structure - Source: Mokhtari et al. (2011)

6.2.2 Event Tree Analysis (ETA)

ETA is a qualitative and quantitative risk assessment technique in which each component of the system, including workers, undergoes evaluation using an inductive approach. This approach starts with an initial event (Andrews and Dunnett, 2000). It provides information on how the failure occurs and the probability of the failure (see Figure 5-3 below).

ETA is a method of tracking the impact of making a distinction between how the safety system works after the initial event occurs: success or failure (Ferdous et al., 2013). The number of events is prepared by listing the components of the system to be analysed, or their functions, in order from left to right, starting with the functions representing the initial failure. ETAs also benefit from graphical representations of failures and

sequences of events, similar to the FTA. It is possible to analyse multiple failure paths, and cause-effect relationships with their dependencies can be displayed.

Additionally, it is capable of assessing probability and detecting insufficient countermeasures (Aust and Pons, 2019). A limitation of the ETA is that it analyses only one initiation event at a time. Therefore, it cannot be used when multiple events must take place simultaneously, as the branches would be redundant. ETA uses binary logic, which makes it difficult to represent scenarios that are uncertain, such as those involving people or the environment. It can represent complex events, though, but they lead to vast and highly multiple diagrams. Simultaneously, disentangling the diagram can result in the removal of subtle dependencies (Rausand and Hoyland, 2003). Figure 6-3 presents the concept of event tree structure.

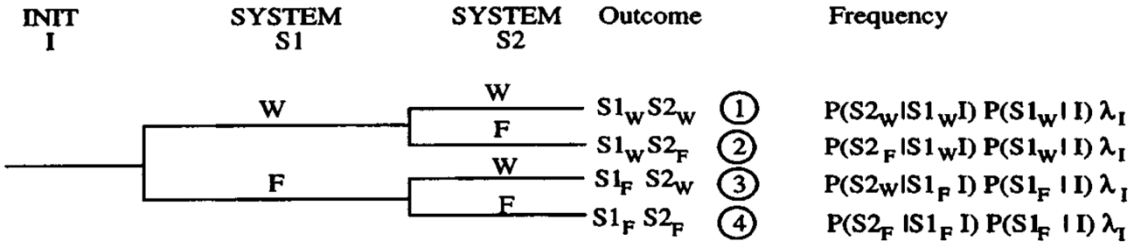


Figure 6-3: Simple event tree structure - Source: Andrew and Dunnett (2000)

6.2.3 Barrier Analysis (BA)

The 'Swiss Cheese Model' of system failure, as presented in Figure 6-4, was conceptualised by James Reason. This model is built upon the concept of 'defence in depth,' where layers of protection, also known as barriers, are represented by slices of Swiss cheese. These layers prevent hazards from materializing and allow consequences to occur (Center for Chemical Process Safety, 2018).

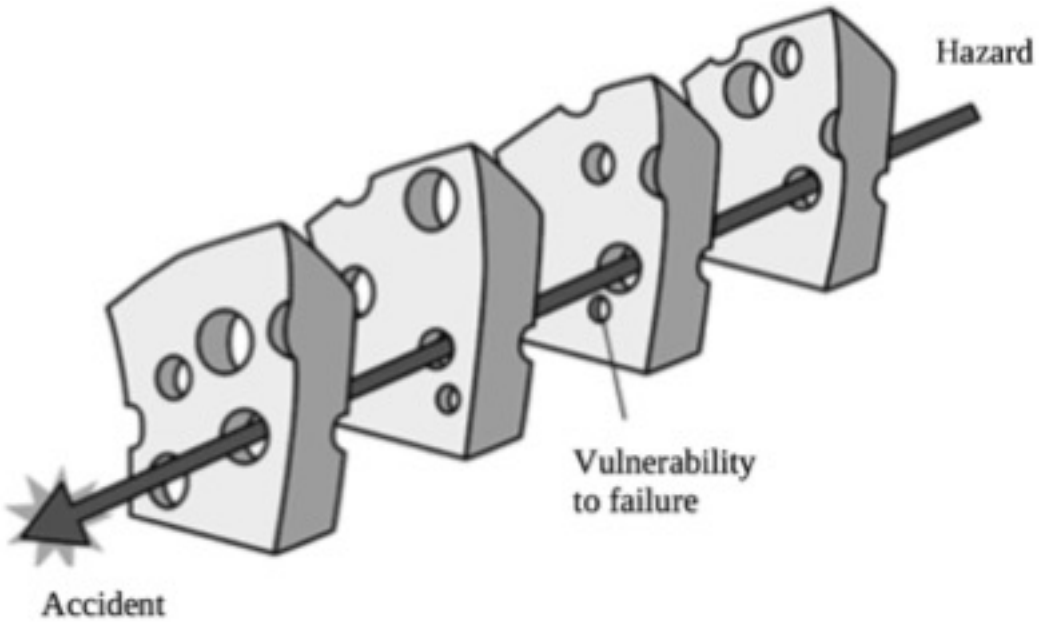


Figure 6-4: Concept of Swiss cheese model - Source: Center for Chemical Process Safety (2018)

Barrier Analysis (BA) is a method used for system safety assessment, enabling the identification of potential risks and the assessment of corresponding controls to prevent incidents. It finds broad application across various domains, including quality, safety, security, and health (Aust and Pons, 2019). BA employs the concept of multiple barriers, which is based on the Swiss cheese metaphor proposed by Reason (1990). In this approach, several barriers are in place so that if one fails, subsequent ones can prevent an event from occurring (Rausand, 2013). This approach is easy to understand as it outlines both the existing barriers and those that could prevent or mitigate an undesired event (Aust and Pons, 2019). However, it is important to note that BA has its limitations as a sole risk assessment tool since it does not account for human errors and hardware failures that are not directly linked to hazardous energy (Ericson, 2011).

6.3 Element of Bowtie Analysis and Structure

The characteristics of each element of the bowtie are described in this section. The bowtie model contains four elements, which will be described in this part; these elements are (1) top event, (2) threats, (3) consequences, and (4) barriers. This is shown in Figure. 6-5.

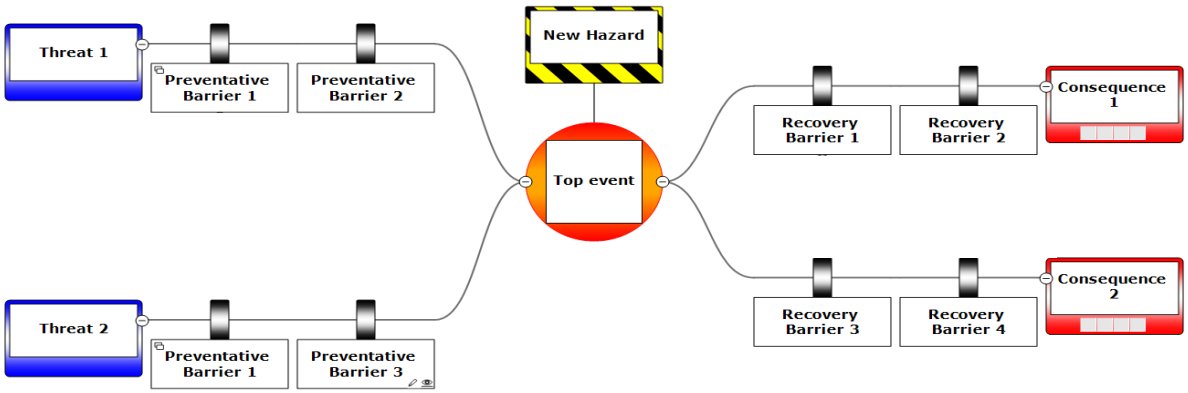


Figure 6-5: Generic structure of a Bowtie diagram

6.3.1 Top Event(s)

Bowtie analysis defines the central event as the moment when there is a loss of control or a loss of risk inhibition between the threat and consequence. In fault tree analysis, important events are situated at the top and referred to as 'Top Events' (de Ruijter and Guldenmund, 2016). This top event signifies the point at which containment or control is compromised, potentially leading to harmful consequences. Even if the top event has occurred, there may still be an opportunity for barriers to mitigate or prevent these consequences. Fault tree analysis places undesirable events at the top of the fault tree, tracing them back to more fundamental faults, and employs logic gates to determine their causes and likelihood (Center for Chemical Process Safety, 2018).

6.3.2 Threats

Threats are potential causes of hazard control failure, leading to the top event. Each top event typically has multiple threats illustrated on the left side of the diagram, each representing an independent scenario that can lead to it (de Ruijter and Guldenmund, 2016; DNV, 2016). When all safety barriers fail, these threats can trigger the top event. There can be one or multiple threats leading to the top event (Aust and Pons, 2019). These threats could act as initiating events, resulting in a loss of control or containment of a hazard (Center for Chemical Process Safety, 2018).

6.3.3 Consequences

The consequences of the top event are the potential outcomes or a sequence of potential outcomes that may lead to damage or loss of control if all mitigation barriers

fail (DNV, 2016). A single top event can have multiple consequences, each of which may have its own set of mitigation barriers to reduce the impact. Typically, in the structure of bowtie diagrams, threats are initially defined on the left side, and then the consideration of consequences follows on the right side (Center for Chemical Process Safety, 2018).

6.3.4 Barriers

In a bowtie system, barriers are positioned along the pathways connecting threats to the top event (referred to as preventative barriers) and between the top event and its consequences (known as recovery barriers). Preventative barriers function to prevent the occurrence of the top event, while recovery barriers are designed to mitigate severe damage in the event that the top event does occur. These pathways may have one or multiple barriers, and multiple barriers are preferable when they can provide contingency measures in case one of them fails (de Ruijter and Guldenmund, 2016).

After identifying the threats and consequences, a bowtie analysis can be built, in which threats that cause the event are presented on the left side, and the potential consequences of the event are listed on the right side (Bernsmed et al., 2017). Figure 5-5 presents an example of a bowtie structure. A top event is first identified in the centre of the structure (i.e., the orange circle), whilst the left side of the structure shows:

- Identified threats (i.e., the blue rectangles) that could lead to the top event.
- Identified preventative barriers (i.e., the black-line rectangles) to prevent a threat from trigging the top event.
- Identified escalation factors (i.e., the yellow rectangles) that restrict or defeat the effectiveness of the preventative barriers as well as the control measures (i.e., secondary level barrier) that limit the negative effect of the corresponding escalation factors.

Meanwhile, the right side of the bowtie structure shows:

- Identified potential consequences (i.e., the red rectangles) following the top event and developed event sequence paths
- Identified recovery barriers to inhibit the escalation from the top event to the potential consequences.
- Identified escalation factors that restrict or defeat the effectiveness of the recovery barriers as well as the control measures that limit the negative effect of the corresponding escalation factors.

6.4 Review of Bowtie Method-related Literature

6.4.1 Advantages of Using Bowtie Analysis

To efficiently manage risk, it is imperative to comprehend all incident pathways and implement control barriers that are both effective and reliable in preventing and mitigating risks (de Ruijter and Guldenmund, 2016; Center for Chemical Process Safety, 2018). Compared to other risk assessment models, such as Quantitative Risk Assessment (QRA), Layer of Protection Analysis (LOPA), Fault Tree Analysis (FTA), and Event Tree Analysis (ETA), bowtie analysis provides a simple and readily understandable visualisation of the relationships between the causes of events leading to a loss of control over threats, potential consequences, prevention barriers, and mitigation barriers for consequences. This makes it easier for people, including non-experts, to grasp the entirety of the risk management process. In other words, a well-developed bowtie method can offer visual benefits to users, simplifying the presentation of both safety and security considerations without overwhelming them with information (Bernsmed et al., 2017; Progoulakis et al., 2021).

Many studies have addressed the advantages of bowtie analysis in risk assessment. With a thorough reviewing relevant literature, this research summarises the following advantages of bowtie analysis, whereas the literature references are listed in Table 6-1.

Visualisation / easy-to-understand

Visualisation is one of the primary advantages of using bowtie analysis, as it allows users to easily grasp the entire landscape of risk management without the need for complex

documentation (Bernsmed et al., 2017). Furthermore, it has the capability to convey a substantial amount of information by unfolding the pertinent layers, such as the responsibilities of barriers and the detailed activities of these barriers, among other factors. This visual representation, encompassing the number and types of barriers and degradation controls, as well as their current state, offers a comprehensive view of risk. Consequently, it enables the identification and prioritisation of degraded barriers and degradation controls (Center for Chemical Process Safety, 2018).

Logical and robust structure

The bowtie analysis can present risk management processes from threats to consequences with a visual image, which is a logical, structured, and incremental manner (Progoulakis et al.,2021). It can demonstrate the process of the link between the top event, threats, barriers, and consequences and explains their causes and effects (de Ruijter and Guldenmund, 2016). It can help to identify gaps in existing control measures, allowing organisations to implement additional measures to mitigate risks and improve their overall risk management strategy (Center for Chemical Process Safety, 2018).

Assistance in developing risk management

Given the advantages of visualisation and the presentation of logical structures, a bowtie analysis could easily adapt and amend existing management systems, and it provides a structured process where identified hazards, threats, and consequences can be related in cause-and-effect scenarios and assist in the development and understanding of how unwanted events can occur (Center for Chemical Process Safety, 2018). At the same time, it can help prioritise the effectiveness of preventative and recovery barriers. Furthermore, with a bowtie analysis, organisations can adhere to regulatory requirements and industry standards by managing risks in a structured and comprehensive manner (Progoulakis et al.,2021).

Promotion of risk awareness for user

The bowtie approach can be applied to educate and enhance awareness of the significance of risk management while aiding users in developing their risk strategies (Aust and Pons, 2019). Through its visual representation of the structure, it can assist in the design, operational, and maintenance processes, promoting awareness and understanding of existing barriers and their operation and maintenance (Turner et al., 2017; Center for Chemical Process Safety, 2018).

Table 6-1: List of literature on the advantages of bowtie analysis

Author / Year	Visualisation	Logical and robust structure	Assistance of development risk management	Promotion of risk awareness for user
Ferdous et al. (2013)	√	√	√	
de Ruijter and Guldenmund (2016)	√		√	
DNV (2016)	√			
Mohr (2016)	√			
Smolarek (2016)	√		√	
Abbassi et al. (2017)	√			
Bernsmed et al. (2017)	√		√	√
Turner et al. (2017)	√	√	√	√
Abdo et al. (2018)			√	
Astles and Cormier (2018)	√	√	√	
Center for Chemical Process Safety (2018)	√	√	√	
Voicu et al. (2018)	√	√	√	√
Aust and Pons (2019)	√	√	√	√
Cormier et al. (2019)				√
Meland et al. (2019)			√	
Mullins et al. (2019)			√	
Aust and Pons (2020)	√		√	
Progoulakis et al. (2021)	√	√	√	√
Alani and Mahjoob (2021)		√	√	
Taleb-Berrouane et al. (2021)		√		
Sheehan et al. (2021)			√	
Uflaz et al. (2021)		√		
Mohd Nizam Ong et al. (2022)		√		

Based on the above discussion about the function and advantages of using bowtie analysis, this chapter will apply this method to illustrate and analyse the risk management process of maritime cybersecurity.

6.4.2 Application of Bowtie Analysis in a Non-maritime Context

Before reviewing the application of bowtie analysis in the maritime industry, a brief review of its applications in other industries is presented. In fact, bowtie analysis has been used for mitigation measures or risk assessment guidelines in different industries; Table 6-2 presents a brief summary of some relevant papers.

The Center for Chemical Process Safety (2018) presents several instances of bowtie analysis application within major regulatory bodies and industries, demonstrating how the bowtie approach is being embraced in the chemical industry. For instance, the American Petroleum Institute (API, 2016) has recommended the use of bowtie analysis for offshore operations. The European Commission, in its report 'Safety of Offshore Oil and Gas Operations Directive' in 2013, highlighted the need for risk assessment and the identification of barriers to prevent accidents and enhance response capabilities. Additionally, the UK Health and Safety Executive (UK HSE, 2013) recognises bowtie analysis as a valuable tool for a barrier-based approach to risk assessment. The COMAH Competent Authority (SEPA, 2016) has incorporated the bowtie method into reports to support the risk assessment of major environmental incidents. Finally, the International Association of Oil and Gas Producers (IOGP) underscores the importance of bowtie diagrams and discusses methods for maintaining and updating barriers in their 2016 reports, numbered 456 and 556 (IOGP, 2016).

Despite the importance of vulnerability consideration in the overall assessment process, quantitative indicators are explicitly omitted from the diagram. The US Coastguard (USCG) referred that cyberattacks on marine transportation systems can be prevented and responded to by using bowtie (Tucci, 2017).

Table 6-2: List of literature on bowtie analysis applied in various industries

Authors (year)	Industry	Brief Summary
Abdo et al. (2018)	Chemical	They integrated an attack tree and bowtie analysis methodology to evaluate both safety and security risks in the industrial environment in the context of cybersecurity.
Astles and Cormier (2018)	Fishery	They sought to integrate bowtie analysis and ecological risk assessment in order to assess fisheries management in Australia. They emphasised that this approach serves as a valuable instrument for engaging stakeholders and communities, rendering the intricacies of fishery management accessible to everyone.
McLeod et al. (2018)	Health care	They addressed that bowtie analysis could be applied as a means of proactively identifying and assessing the controls to serious significant events in primary healthcare.
Aust and Pons (2020)	Aerospace	They discussed a novel conceptual framework for visually inspecting gas turbine components. This framework was introduced by merging the bowtie method with Ishikawa's 6M structure to categorise threats, consequences, and barriers.
Bensaci et al. (2020)	Robot engineering	They integrated System-Theoretic Process Analysis (STPA) and bowtie analysis for the purpose of safety assessment. Their method provides a comprehensive means of identifying hazards for autonomous multi-mobile robots.
Mohammadfam et al. (2020)	Chemical	They utilised bowtie analysis within a Bayesian network and carried out a cause-consequence analysis concerning material leakage from trucks. Their investigation involved examining the fundamental and intermediary events related to chemical leakage from trucks in historical accidents. Additionally, they explored the parameters influencing the occurrence of these consequences and the nature of the consequences through the application of bowtie analysis.
Aust and Pons (2020)	Aerospace	They proposed that the bowtie diagram provides new insights into the consequences of visual inspection in aircraft engine maintenance. As a result, certain controls in the workflow are understood in a new light.
Sarvestani et al. (2021)	Chemical	They employed the bowtie method to ascertain the critical event, prevention, and damage control measures for incidents involving LP gas tanks. Through the combined use of the MIMAH method and Bayesian theory, they pinpointed that the most crucial barrier in averting accidents is the prevention of gas release.
Yang et al. (2021)	Chemical	They devised a unifying approach to simultaneously assess safety and security risks in chemical industrial applications and cyber-physical systems. Their method integrated the bowtie analysis technique and security assessment by scrutinizing preventive measures and barriers.

6.4.3 Bowtie Analysis in the Maritime Industry

Although bowtie analysis has been applied in several industries, there are only a few studies related to actual industrial applications. Notably, DNV has extensively applied the bowtie methodology. For instance, in DNV's report from 2016, they propose the use of bowtie analysis (see Figure 2-7 in Chapter 2) for assessing maritime cybersecurity. This involves first identifying potential cyber threats and their consequences, such as unauthorised access to sensitive information or disruption of critical systems. Subsequently, they identify the barriers and controls that could prevent these threats, including firewalls, anti-virus software, and employee training. They also identify potential failures or weaknesses in these barriers and controls. Finally, they develop additional controls and contingency plans to mitigate the consequences of these failures.

Regarding academic publications, the literature is rather scant. Yang (2011) assessed maritime security risks and developed risk management strategies for maritime supply chains in Taiwan. Abbassi et al. (2017) assessed the causes and consequences of vessel navigation accidents in the Arctic Ocean. Voicu et al. (2018) addressed risk assessment with several cases of oil spills from vessels. Fjørtoft and Mørkrid (2021) investigated the resilience mechanism of autonomous shipping. They found resilient systems and situational awareness are significant elements of autonomous vessel systems.

In the research area of vessel navigation, Trbojevic and Carr (2000) applied barrier bowtie models to analyse the risks and hazards for improving port safety in the hopes of reducing navigation errors and vessel incidents. King et al. (2016) stated that extreme weather, incorrect loading and fire water accumulation could be threats to navigational accidents of large passenger vessels. Abbassi et al. (2017) used bowtie analysis to investigate the relationship between vessel accident causes and consequences in the Northern Sea Route. They addressed that cold and harsh conditions affect vessel navigating, and grounding and foundering can occur as a result. Arici et al. (2020) focused on ship-to-ship (STS) cargo operations' risk assessment by applying fuzzy bowtie analysis, including several consequences such as loss of life, marine pollution, a capsizing.

Progoulakis et al. (2021) analysed the interconnections among marine equipment, systems, and processes onboard in the case of safety incidents.

In the area of maritime environmental protection, Cormier et al. (2019) addressed environmental protection strategies with marine risk management. According to their research, the use of IEC/ISO 31010 bowtie analysis can serve as a valuable instrument in comprehending and addressing the diverse array of environmental pressures that affect the marine ecosystem by establishing an organised and integrated approach towards decision-making in this context. Sotiralis et al. (2019) analysed the causes and consequences of maritime environmental accidents and argued that omissions during the inspection process are a significant factor that contributes to the occurrence of maritime accidents. Subagyo et al. (2021) investigated the risk of oil and gas pipeline spills in the Indonesian Sea and found that risk levels are different when pipelines are placed in different locations (e.g., onshore, shallow water and high sea) even using the same risk factor. Bayazit and Kaptan (2023) assessed the risk of marine pollution caused by ship operators by applying a hybrid method called bowtie analysis based on Fuzzy Bayesian Networks.

In addressing cyber-physical security Bernsmed et al. (2017) conducted an analysis and visualisation of physical and cyber security risks. They provided an example related to navigational communication systems within the maritime industry. Progoulakis et al. (2021) illustrated an example involving malware contamination of a vessel's engine human-machine interface (HMI) system. In their research, they identified consequences such as 'Incorrect engine operational parameters' and 'Engine malfunction or stoppage.' In a separate study, Fjørtøft and Mørkrid (2021) delved into the mechanisms of resilience in autonomous shipping, using bowtie analysis. Their findings underscored the critical importance of resilient systems and situational awareness as essential components for the successful operation of autonomous vessel systems.

6.5 A Bowtie-based Framework for Maritime Cybersecurity Risk Assessment

Bowtie analysis can serve as a valuable framework for assessing cybersecurity risks, as illustrated in Figure 6-6. According to DNV (2016), which proposed maritime cybersecurity risk assessment using bowtie analysis, the process begins with the identification of the scope. This determination is company-specific and plays a crucial role in defining the analysis boundaries. Conducting a literature review or interviews with experts and end users can be valuable in this phase. The primary focus here is on identifying relevant hazards. Since a single bowtie analysis typically covers a single hazard, it is essential to perform multiple analyses to address all pertinent hazards.

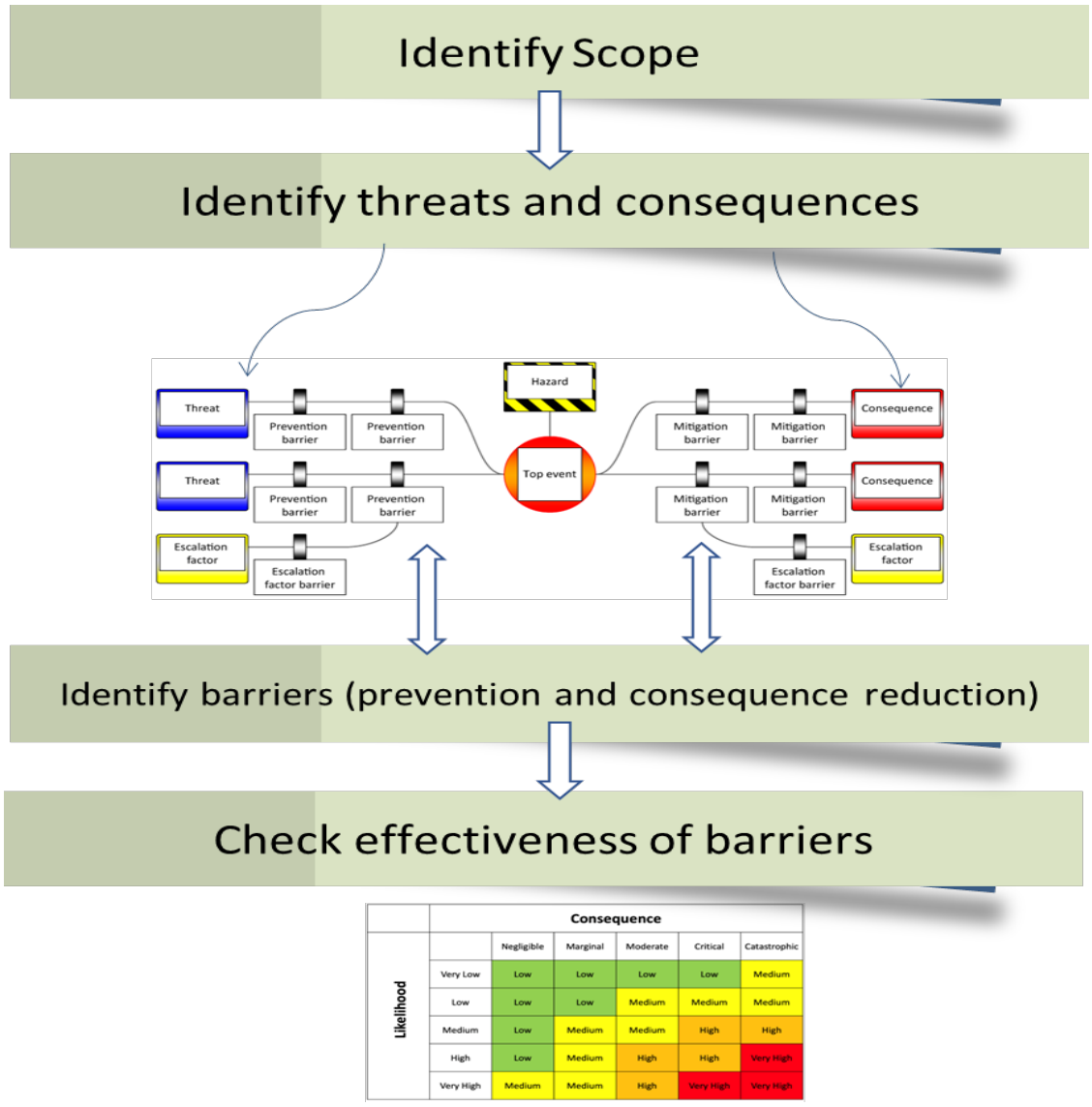


Figure 6-6: Bowtie-based Framework for Cybersecurity risk assessment

For each hazard, a bowtie diagram is employed to depict the relevant causes and threats. To identify the appropriate barriers, a systematic process should be followed. According to ISO 31010, *'this information may be obtained from the results of risk and control identification techniques or from the expertise of individuals.'* In practice, bowtie diagrams are frequently created directly by a team in a workshop setting.

"The next step involves analysing the effectiveness of the barriers. To do this, it is essential to assess the current risk level without the presence of the barrier, which can be done using qualitative or semi-quantitative methods. Risk matrices, as discussed in Section 5.5.1 below, can be particularly useful for this purpose. Afterward, an evaluation of the risk reduction, which involves assessing the risk level following the implementation of the barrier, can be carried out. This evaluation helps in gauging the effectiveness of the barriers, and they can be ranked based on their effectiveness.

This is a very simplistic approach that can be used for a high-level analysis or at an initial stage, especially where a qualitative approach is desirable. There are several advantages associated with the bowtie analysis, as presented in Section 6.4.1.

However, this cannot be used in situations where pathways from causes to the event are not independent, and it can oversimplify complex situations where quantification is needed. There is also an issue with the combination of different aspects of consequences. In this case, a multi-objective approach using, for example, the methods presented in Chapter 3 (e.g., TOPSIS) is the preferable solution.

6.5.1 Risk Matrix

In bowtie analysis, each risk can be measured in a quantitative or qualitative way using a risk matrix. A risk matrix is typically presented as a chart or table with two axes representing likelihood and consequence levels. In its simplest qualitative form, the likelihood of a risk is usually evaluated using a scale of low, medium, and high, while the consequence of a risk is assessed using a scale of negligible, moderate, and catastrophic

(Alyami et al., 2019; Chang et al., 2021). The risk value is calculated as the product of the two (i.e., likelihood and consequences).

	Consequence					
Likelihood		Negligible	Marginal	Moderate	Critical	Catastrophic
	Very Low	Low	Low	Low	Low	Medium
	Low	Low	Low	Medium	Medium	Medium
	Medium	Low	Medium	Medium	High	High
	High	Low	Medium	High	High	Very High
	Very High	Medium	Medium	High	Very High	Very High

Figure 6-7: Example of Risk matrix - Source: Author

Risk matrices have found widespread application across various industries, including manufacturing (Albery et al., 2016; Ratnayake and Antosz, 2017), oil and gas (Lu et al., 2015; Luo et al., 2018), construction (Mahamid, 2011; Qazi et al., 2021), healthcare (Arnetz et al., 2014; Pascarella et al., 2021), transport, and others (Skorupski, 2016; Wan et al., 2019a). The concept of a risk matrix is visually illustrated in Figure 6-7. The degree of likelihood and consequence can be adjusted based on specific circumstances. For instance, they may be categorised into three levels (Low, Medium, High) (Arnetz et al., 2014; Albery et al., 2016) or five levels (Very Low, Low, Medium, High, Very High) (Pascarella et al., 2021; Qazi et al., 2021).

Risk acceptance criteria can also be incorporated; see the different colours in the matrix below. Green colour refers to low risk, Yellow colour means medium risk, and Red colour high risk (Cox, 2008; Park et al. 2023).

Note here that there has been a wide use of risk matrices in qualitative and semi-quantitative approaches in various industries; see references above. The risk matrix should reflect the company, national and international regulations and practices and should be suitable for the specific assessment needs.

"In this study, consideration is proposed for four categories when assessing the consequences (impact). These categories align with various industrial approaches and are illustrated in Table 5-3. They follow the widely adopted PEAR framework, which encompasses People, Environment, Assets, and Reputation. For an example of a risk matrix, please refer to Figure 6-8, as presented in ISO standard 16901:2022, titled 'Guidance on performing risk assessment in the design of onshore LNG installations, including the ship/shore interface'.

Consequence					Increasing probability			
Severity rating	People	Assets	Environ-ment	Repu-tation	A	B	C	D
					Has occurred in E&P industry	Has occurred in operating company	Occurred several times a year in operating company	Occurred several times a year in location
0	Zero injury	Zero damage	Zero effect	Zero impact	Manage for continued improvement			
1	Slight injury	Slight damage	Slight effect	Slight impact				
2	Minor injury	Minor damage	Minor effect	Limited impact				
3	Major injury	Local damage	Local effect	Conside-rable impact				
4	Single fatality	Major damage	Major effect	Major national impact	Incorporate risk-reducing measures		Fail to meet screening criteria	
5	Multiple injury	Extensive damage	Massive effect	Major international impact				

Figure 6-8: Example of Risk matrix - Source: ISO 16901:2022 (ISO, 2022 b)

Table 6-3 provides a compilation of literature relevant to the four aspects mentioned earlier. It is important to note that integrating these various aspects into a single risk assessment can be a complex task. One approach is to assign monetary values to all

consequences, including safety and environmental impacts. Another viable method involves employing a multi-attribute analysis.

Table 6-3: List of papers related to the risk matrix dimensions

Aspect of Consequence	Reference/Source
People	Mraković and Vojinović (2019), Farah et al. (2022)
Assets	Abdo et al. (2018), Alcaide and Llave (2020), Sheehan et al. (2021), Bolbot et al. (2022), GOV UK (2022), Kayisoglu et al. (2022), Kanwal et al. (2022), Żebrowski et al. (2022), Afenyo and Caesar (2023)
Reputation	Alcaide and Llave (2020), Couce-Vieira et al. (2020), De Peralta et al. (2020), Senarak (2020), Ghadiminia et al. (2021), Kechagias et al (2022), Jones et al. (2016), Meland et al. (2021), Kanwal et al. (2022)
Environment	Boyes (2014), Jones et al. (2016), Bolbot et al. (2020), Sepehri et al. (2022)

Safety (People)

Cyberattacks in the maritime context can pose significant risks to human safety (Mraković and Vojinović, 2019; Farah et al. 2022). If attackers gain access to a vessel's critical systems, they can manipulate them to cause equipment malfunctions, steer the vessel off course, or even shut down the vessel's engines, potentially resulting in collisions or groundings (Farah et al. 2022). In addition to these direct risks, a cyberattack can compromise the vessel's ability to communicate with onshore facilities and emergency responders, leading to delayed or inadequate responses to critical situations like medical emergencies or accidents. Furthermore, a cyberattack may impact the vessel's safety equipment, including life-saving appliances, fire extinguishing systems, and emergency power supplies.

Asset

Cyberattacks can have a profound impact on various assets, including important data, financial assets, and physical assets (Alcaide and Llave, 2020; GOV UK, 2022). A notable case in the maritime sector is Maersk, which reportedly spent an estimated $200-300 million USD to recover its systems after a cyberattack. In this research, financial loss encompasses not only the direct recovery costs but also additional expenses and income

reductions resulting from cybersecurity incidents. These may include financial asset losses, increased insurance costs, reduced income, and other related factors (Kanwal et al., 2022). Kanwal et al. (2022) further argue that the growing threat of cyberattacks on vessels and their potentially catastrophic consequences can significantly impact the financial aspects of shipping companies. For instance, the malfunction of essential systems like SCADA can lead to financial losses (Abdo et al., 2018; Żebrowski et al., 2022). Therefore, they advocate the importance of emphasizing efficient cybersecurity practices to enhance the cybersecurity performance of ships.

Reputation

Cyberattack incidents have the potential to harm an organisation's reputation and erode trust among customers and suppliers, which can significantly impact the company's long-term profitability and viability (Couce-Vieira et al., 2020; Ghadiminia et al., 2021; Kechagias et al., 2022). Couce-Vieira et al. (2020) emphasise that organisational reputations are more directly influenced by factors that affect brand value, reduce income and operational efficiency, or necessitate efforts to rebuild reputation, rather than factors that are directly measurable. Ghadiminia et al. (2021) assert that malicious access can expose organisations to reputational losses. In the maritime context, Jones et al. (2016) highlight that maritime cyberattacks can harm the reputation of shipping lines and maritime organisations. Furthermore, both Meland et al. (2021) and Kanwal et al. (2022) point out that cyberattacks on ships can have devastating consequences that also impact the reputation of shipping companies.

Environment

Cybersecurity incidents within the maritime domain have the potential to significantly impact the marine environment (Boyes, 2014; Jones et al., 2016; Bolbot et al., 2020). This is primarily because hijacked vessels may carry hazardous materials, dangerous chemicals, or oil rigs, and a cyberattack can result in pollution. Oil spills, in particular, can have adverse effects on fisheries and aquaculture systems. Furthermore, a security breach targeting a ship's navigational infrastructure could lead to collisions and

accidents, thereby jeopardizing the safety of the vessel, compromising its cargo, and causing harm to the marine ecosystem (Sepehri et al., 2022).

6.6 An Illustrative Example of an Application of a Bowtie Framework for Maritime Cyber Security Analysis

This Section will illustrate the cyber risk assessment approach using the bowtie analysis for a cyber hazard that has been identified in Chapter 4, namely the one related to Malware. A number of threats, see Section 6.6.2, have been identified in Chapter 4. Consequences are presented in Section 6.6.3 below. Relevant barriers (or risk control options) have been identified in Chapter 5; here, barriers more specific to the Malware hazard are presented in Section 6.6.4.

6.6.1 Top Event and Relevant Hazard

In this chapter, Malware will be used as a case study to illustrate the bowtie framework for maritime cybersecurity, given its top-ranked position in Chapter 3. Malware refers to malevolent software that infiltrates and compromises devices without the user's awareness. It propagates itself by downloading attached files from infected emails, exploiting vulnerabilities through interaction with counterfeit websites, or establishing connections with USB drives and other removable media, including malicious code (Pham et al., 2010).

6.6.2 Threats

The Malware category includes the following five threats:

- Mal1: Accessing links from suspicious emails,
- Mal2: Downloading attached files from unknown emails,
- Mal3: Connecting USB or removable media to computers/equipment without virus check,
- Mal4: Connecting your infected USB or removable media to connect computers/navigation systems,
- Mal5: DDoS attacks company's server system

6.6.3 Consequences

OT System (e.g., ECDIS) unavailable

Cyber attackers may deploy malware to disable or disrupt critical operational systems on vessels and in ports, rendering them temporarily or permanently unavailable (Bolbot et al., 2019). The unavailability of these systems can have serious repercussions for vessels, their crews, and their cargo (BIMCO, 2018). In some instances, attackers may aim to gain unauthorised access to systems and tamper with or delete critical data, further hindering the proper functioning of these systems (BIMCO, 2018; Meland et al., 2021; Akpan et al., 2022). Moreover, cyberattacks can affect emergency responders by targeting navigational and operational technology (OT) systems, including the Automatic Identification System (AIS), Electronic Chart Display Information System (ECDIS), Global Navigation Satellite System (GNSS), Global Positioning Systems (GPS), and Industrial Control Systems (ICSs). Such attacks can lead to incidents like ship hijacking due to loss of GPS control (Akpan et al., 2022; GOV.UK, 2022). The limited availability of technical support and resources at sea exacerbates the impact of a network outage resulting from a cyberattack (Mraković and Vojinović, 2019). Depending on the severity and consequences of the attack, the affected systems may require repairs, updates, or even replacement to restore functionality, incurring significant costs and causing delays.

Data breach

Data breaches within the maritime domain occur when an unauthorised party gains access to sensitive information stored on a vessel's computer systems or networks (BIMCO, 2018; Park et al., 2019). These breaches can inflict financial and reputational damage on maritime companies due to the theft or alteration of critical data, including personal information of crew members and cargo manifests. Such breaches also pose risks to the vessel's operations, safety, and financial stability (Jones et al., 2016; Progoulakis et al., 2021). Stolen data can be exploited for various malicious purposes, including identity theft, ransom demands, or targeted attacks on the vessel or its cargo (Kuhn et al., 2021). In some cases, attackers may attempt to disrupt the vessel's operations by manipulating critical systems, such as navigation or engine controls.

IT/ICT disruption

IT/ICT disruptions resulting from cyberattacks can lead to communication delays between vessels and/or port authorities, posing significant safety concerns (DiRenzo et al., 2015; Jones et al., 2016). For instance, disruptions to GPS signals, which have multiple points of failure, can result in misunderstandings in communication between ships and ports or between ships themselves. This can affect a vessel's navigation, cause communication breakdowns with other vessels, and lead to cargo movement delays (Kala and Balakrishnan, 2019). Moreover, miscommunication between vessels and ports or among vessels can result in incorrect courses, potentially leading to collisions or accidents and unsafe conditions for workers and the public (Alcaide et al., 2020). Ships may have limited bandwidth and connectivity, making it challenging to obtain necessary software updates or communicate with onshore support teams (Boudehenn et al., 2021). Furthermore, ICT disruptions can disrupt email and marine traffic control systems, as demonstrated by incidents such as those at the San Diego port and the Port of Barcelona in 2018. The literature listed of consequence are shown in Table 6-4.

Table 6-4: List of Consequences

Consequences	Reference/Source
OT systems unavailable	Bolbot et al., (2019), BIMCO (2018), Mraković and Vojinović (2019), Meland et al. (2021), Akpan et al (2022), GOV UK (2022)
Data breach	Jones et al. (2016), BIMCO (2018), Park et al. (2019), Progoulakis et al. (2021), Kuhn et al. (2021)
IT/ICT disruption	DiRenzo et al. (2015), Jones et al. (2016), Kala and Balakrishnan (2019), Boudehenn et al. (2021),

6.6.4 Barriers

A number of preventative and recovery barriers are identified from relevant studies that can be adopted for maritime cybersecurity. The detail of the barriers is presented as follows:

Preventative barriers

Up-to-date anti-virus software

One of the most effective approaches to mitigating cyberattacks is to utilise anti-virus software, which should be regularly updated to the latest version (Fitton et al., 2015; Lagouvardou, 2018). Given the rapid advancement of technology, many viruses and malicious programs are being developed concurrently, making it necessary to employ protective measures to safeguard against unauthorised access to sensitive information, data breaches, network connectivity losses, and the risk of DDoS attacks (Sheehan et al., 2021). Despite the potential recovery benefits of this method, it can also act as a barrier, providing early detection and quarantine capabilities in the event of a cyberattack. In the shipping industry, both BIMCO (2018) and Progoulakis et al. (2021) recommend that anti-virus software should be installed on all work-related computers aboard vessels to reduce the likelihood of cyberattacks.

Strong password policy

The mandated use of complex passwords, coupled with regular password changes, is widely acknowledged as a cost-effective and readily executable measure against cyber threats (National Cyber Security Centre, 2019). In the shipping industry, the absence of a password management policy has resulted in 40% of crew members sharing passwords for accessing onboard systems (Alcaide and Llave, 2020). Consequently, a robust password policy is recommended to address the threat of unauthorised access (IMO, 2021). This may entail proscribing the practice of storing individual passwords on shared systems, sharing passwords among colleagues, and mandating periodic password changes (Koola, 2018). Furthermore, maritime cybersecurity can be further enhanced by utilizing multi-factor authentication (BIMCO, 2018).

VPN/Firewalls

Most devices/systems do not operate in isolation; they communicate with each other and can be accessed from the "outside" world. Network devices configuration such as the use of proxy servers, encryption, firewalls, and Virtual Private Networks (VPN) are countermeasures for network protocol attacks and could be determined which systems should be attached to controlled or uncontrolled networks to prevent any security risks through connected devices (Jang-Jaccard and Nepal, 2014; Boyes and Isbell, 2017). Network systems that should be placed on controlled networks include networks that are used to provide suppliers with remote access to OT software and networks that are necessary for the operation of a vessel. Misconfigured firewalls and proxy servers can cause errors in network systems onboard vessels and ashore (BIMCO, 2020).

Restricting system access

The interconnected nature of all ship systems makes it possible for only one compromised system to allow access to all other systems. In a ship, all systems are interconnected, so if only one system is compromised, attackers can gain access to everything else. (Akpan et al., 2022; GOV.UK, 2022 Therefore, restricting access to both IT and OT systems can serve as an important countermeasure against specific attacks. Access to these systems should be limited to authorised personnel, enhancing the security of the IT/OT infrastructure.

Education and training

Education and training can play a crucial role in reducing cybersecurity risk in the maritime industry. It is imperative that developing comprehensive cybersecurity training for sea crews and staff could enhance maritime cybersecurity (Jones et al., 2016; Senarak, 2021; Progoulakis et al., 2021; Corallo et al., 2022). Training programs should cover all aspects of cybersecurity and should be mandatory for all employees who have access to sensitive information or critical systems. At the same time, conducting cybersecurity drills regularly can help identify vulnerabilities and ensure that employees know how to respond to a cyber incident (Progoulakis et al., 2021). In the absence of cybersecurity training, the human factor poses a potential threat to maritime and

environmental cybersecurity, which under certain circumstances, could pose a serious problem (Pseftelis and Chondrokoukis, 2021).

Enhancing cybersecurity awareness

A lack of cybersecurity awareness may benefit attackers seeking to gain access to a vessel's systems, steal sensitive information, or disrupt operations. Increasing cybersecurity awareness can empower stakeholders to recognise common cyber threats faced by the maritime industry, such as malware, phishing, and other cyber threats. There is a critical need in the maritime industry to enhance awareness and understanding of actual cyber risks (Karahalios, 2020). The most effective way to reduce cybersecurity incidents is to promote a cybersecurity culture, which includes a cybersecurity awareness campaign and certification for all stakeholders involved in vessel operations (crew, third parties, ports, operators) (BIMCO, 2018).

Cybersecurity policy

Kechagias et al. (2022) proposed several measures to mitigate cybersecurity risks. According to their suggestions, implementing a cybersecurity policy can significantly reduce cybersecurity incidents. The use of procedure manuals and a cybersecurity policy manual can provide a secure method for safeguarding various cybersecurity policies, including those related to hiring and termination, separation of duties, data classification, account disablement, access rights, business contingency plans, incident response plans, third-party management, and more (BIMCO, 2018).).

Recovery Barriers (or consequence mitigation barriers)

Backup data

In case of a cyberattack incident, backup data allows shipping companies to continue working without interruption from the lost data. Particular attention should be paid to the backup data location in this process (DNV, 2016; Kabir et al. 2020). At the same time, it is essential for the stakeholders to back up all critical files, software, and data to minimise recovery time (Kaspersky, 2020). Progoulakis et al. (2021) addressed vessels' engine human-machine interface (HMI) and proposed building redundancy systems as

a recovery barrier to mitigate the impact of HMI data being cyberattacked. Therefore, important data must be backed up by another source to ensure cybersecurity.

Removing virus using anti-virus software

DNV (2021) states that the detection of malware attacks by anti-virus software can reduce the consequences of cyberattacks. They address that in order to safeguard against malware threats, including those that may arise within the context of limited data traffic and bandwidth on ships, it is essential to utilise anti-virus and anti-spyware software with regularly updated signatures.

Furthermore, the implementation of system hardening, and patch management protocols serve as critical barriers against malware, particularly for those systems deemed to be of utmost importance. As such, rigorous testing of any changes made to these critical systems is essential in ensuring optimal levels of security.

Disconnecting System

Disconnecting the affected system can serve as a preventative measure in the context of cyberattacks, as it can limit the attacker's ability to manipulate safety-critical systems or directly control the system. Moreover, disconnecting can also be effective in containing the spread of malware between different network segments. (DNV, 2016; BIMCO, 2018).

Reporting cybersecurity authorities

Alharbi et al. (2021) addressed that contact with cybersecurity authorities and having an inspection team were found to have statistically significant effects on restoration time. The third part, cybersecurity authorities or national cybersecurity authorities must be contacted in many cybersecurity frameworks, especially when mid-level or highly classified security breaches occur. The cybersecurity authorities would give some advice about cybersecurity risks or consultation, guidelines, and regulations for cybersecurity (GOV UK, 2022). The literature listed of Preventative and Recovery barriers are presented in Table 6-5.

Table 6-5: List of Preventative and Recovery Barriers

	Barriers	Maritime-related references
Preventative	**Up-to-date anti-virus software**	Fitton et al. (2015), DNV (2016) Lagouvardou, (2018), Hareide et al. (2018), BIMCO (2018), Progoulakis et al. (2021), Sheehan et al. (2021), Kechagias et al. (2022).
	Strong password policy	DNV (2016), IMO (2018), BIMCO (2018), Alcaide and Llave (2020), Gunes et al. (2021), Kechagias et al. (2022).
	VPN/Firewalls	Jang-Jaccard and Nepal (2014), Boyes and Isbell (2017), (BIMCO, 2020), Gunes et al. (2021), Enoch et al.(2021), Kechagias et al. (2022).
	Restricting system access	DNV (2016), Svilicic et al. (2019b), Akpan et al. (2022), GOV.UK (2022), Kechagias et al. (2022).
	Education and training	Jones et al. (2016), DNV (2016), Svilicic et al. (2019a), Sviicic et al. (2019b), Otto (2020), Senarak (2021), Progoulakis et al. (2021), Gunes et al. (2021), Yoo and Park (2021), Corallo et al. (2022), Kechagias et al. (2022).
	Enhancing cybersecurity awareness	DNV (2016), BIMCO (2018), Sviicic et al. (2019a), Sviicic et al. (2019b), Karahalios (2020), Kechagias et al. (2022).
	Cybersecurity policy	Kalogeraki et al. (2018a), BIMCO (2018), Gunes et al. (2021), Yoo and Park (2021), Kechagias et al. (2022).
Recovery / Consequence mitigation	**Back up data**	DNV (2016), Kabir et al. (2020), Kaspersky (2020), Progoulakis et al. (2021), Kechagias et al. (2022).
	Anti-virus software alarms	DNV (2016), BIMCO (2018), Sheehan et al. (2021), Kechagias et al. (2022).
	System disconnection	DNV (2016), BIMCO (2018).
	Report cybersecurity authorities	Alharbi et al. (2021), Gunes et al. (2021), Kechagias et al. (2022), GOV UK (2022).

6.6.5 Risk Matrix for the Effectiveness Analysis

In this illustrative example, a risk matrix will be employed for one of the four categories (People, Environment, Assets, and Reputation) discussed in Section 6.5.1. The example matrix here is related to the impact on reputation; see Figure 6-9. The risk categories in this qualitative approach are represented by different colours:

- Green indicates “no impact.”
- Yellow indicates “incorporate risk reduction measures.”
- Orange indicates “manage for continuous improvement.”
- Red indicates “intolerable” risk.

Figure 6-9: Risk Matrix of Reputation

6.6.6 Application of the Framework

How the approach in this research works will now be illustrated, with a portion of the pertinent analysis being presented to address risks related to the threat of malware. A simplified bowtie, which has as a top event a malware attack, is presented in Figure 6-10

The left side of Figure 5-10 shows five identified cyberthreats:

- Accessing links from suspicious email (Mal1)
- Downloading attached files from unknown emails (Mal2)
- Connecting USB or removable media to computer without virus check (Mal3)
- Connecting your infected USB or removable media to connect computers/navigation systems (Mal4)
- DDoS attacks company's server system (Mal5)

The right-hand side of the model shows three potential consequences of a malware attack, such as:

- OT systems becoming unavailable
- Data breaches
- IT/ICT disruption

Each of the threats is associated with a number of preventative barriers, which serve as control measures aimed at mitigating the potential impact of the threat. For example, five preventative barriers that could prevent a malware attack due to Mal1, include:

- Education and training
- Using up-to-date anti-virus software
- Enhancing cybersecurity awareness
- Implementing a strong password policy
- Restricting access to reduce spread of malware

There are also several barriers to reducing the consequences. For example, a potential barrier to OT systems becoming unavailable is to back up OT data, remove the virus using anti-virus software, and disconnect the system. A barrier to a data breach is regular backups of the database, removing the malware/virus using anti-virus (or anti-malware) software, disconnecting the OT system, and reporting the accident to cybersecurity authorities. Potential barriers to an IT/ICT disruption are regular data backups, removing the malware/virus using anti-virus software, and disconnecting the IT/ICT system.

Having identified the threats, consequences and barriers, the last step is to assess the effectiveness of these barriers. This is done using the risk matrices. A qualitative approach is intended to be employed in the scenario outlined below. Following the example bowtie, ‘Accessing links from suspicious email (Mal1)’ can lead to having our systems affected by Malware, and this would lead to a data breach.

Suppose that the current risk level has a probability of 'Possible' and a possible impact that has been assessed as 'Limited impact'; these lead to a risk on reputation that falls into the "Incorporate Risk reduction measures" category as illustrated C3 in Figure 6-9.

Now, a measure to reduce the consequence of data breach is to use an anti-virus/anti-malware solution that can, supposedly, totally eliminate the impact. Here, the assumption is made that the probability of a data breach will not be affected by the implementation of this control measure.; therefore, the overall risk on reputation falls now into the ‘no impact’ category (see C1 in Figure. 6-9). Similar assessments should be performed for all risk categories and risk control measures under consideration.

Obviously, the above is an oversimplification as even in a qualitative approach; there is a need to assess likelihoods and consequences. Our example, though, illustrates how the risk assessment framework could work; there is a need for clearly defined risk matrices.

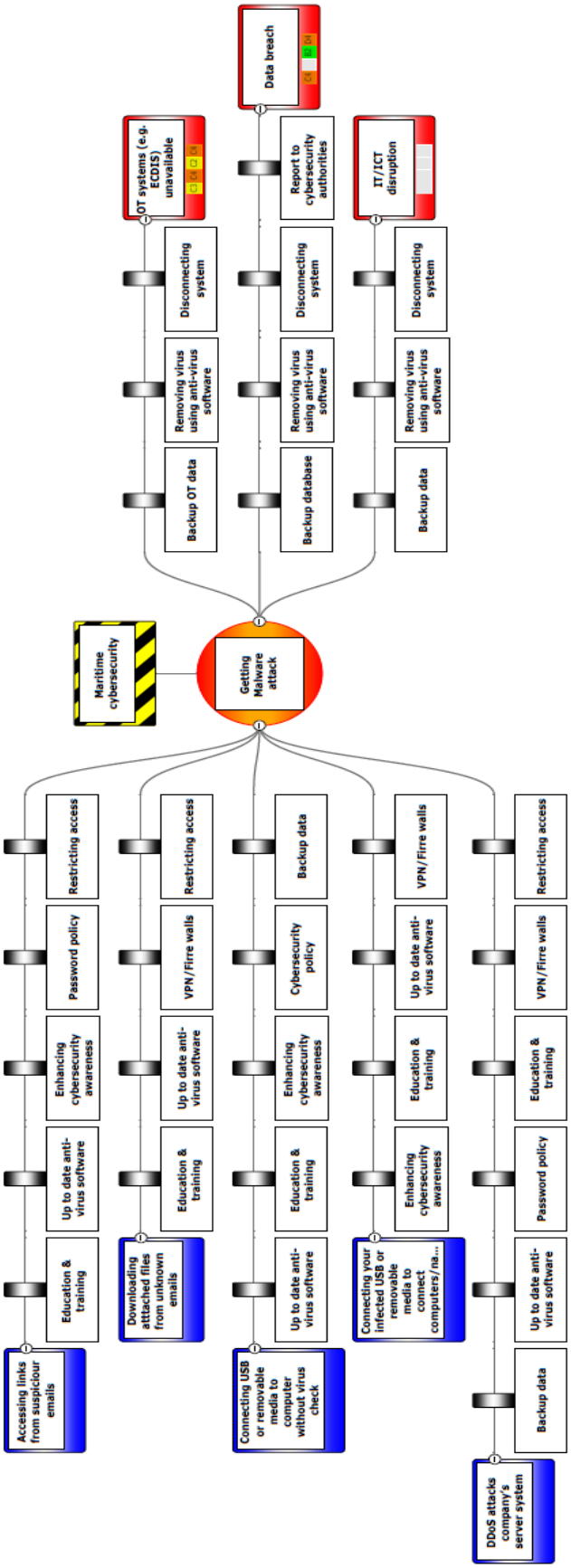


Figure 6-10: Bowtie framework of 'Malware'

6.7 Conclusions and Suggestions for Future Work

This chapter introduces a robust and systematic framework designed for assessing the cybersecurity status within the maritime sector. This assessment is carried out through a carefully selected case study, focusing specifically on the Malware case identified as the primary event in the results of Chapter 3. To conduct this assessment, the framework utilises the well-established and effective Bowtie Analysis methodology.

The main goal of this chapter is to present a comprehensive and structured approach for evaluating cybersecurity in the maritime context. The framework follows a systematic process that includes various stages of analysis and evaluation. Initially, the framework identifies risk control measures relevant to maritime cybersecurity through a meticulous bowtie analysis. A key aspect of this framework is its focus on assessing the effectiveness of these identified risk control measures, which is done through the application of a risk matrix. The risk matrix offers a structured and quantitative way to evaluate how well these measures mitigate potential cybersecurity risks. The combination of bowtie analysis and risk matrix evaluation provides a comprehensive understanding of the strengths and weaknesses in the maritime cybersecurity framework.

An important aspect of this chapter is its commitment to improving accessibility and clarity. By leveraging the analytical capabilities of bowtie analysis and incorporating visualisation techniques, the framework provides a visually intuitive representation of the maritime cybersecurity landscape. This visual representation serves as a powerful tool for understanding various cybersecurity threats in the maritime sector and their potential consequences. Furthermore, it helps stakeholders grasp the intricate implications and possible outcomes associated with cybersecurity attacks. Additionally, the framework is adaptable and versatile, offering a robust qualitative approach suitable for both initial assessments and high-level analyses. This flexibility caters to the varying needs of stakeholders, whether they require a preliminary understanding or a comprehensive evaluation of maritime cybersecurity.

However, there are a few limitations to this framework that could be addressed in future studies especially incorporating the methods presented in Chapters 4 and 5. As it is mentioned earlier in Section 6.5, this approach (using bowtie diagrams) cannot be used in situations where pathways from causes to the event are not independent, and it can oversimplify complex situations where quantification is needed. There is also the need to have separate diagrams for each identified hazard. Another issue is the combination of different aspects of consequences using the risk matrices. In this case, a multi-objective approach using, for example, the methods presented in Chapter 4 (e.g., TOPSIS) is the preferable solution. Note, though, that there is academic literature, see, for example, Cox (2008), that opposes the use of risk matrices altogether due to several limitations.

Furthermore, blockchain technology stands out as a potential future option for risk control. The application of blockchain technology to the maritime industry has been a longstanding consideration. Notably, Maersk previously introduced blockchain technology services, yet extensive research underscores its significance. Blockchain technology offers the potential to alleviate cyber risks through decentralised structures, consensus protocols, and cryptographic hashing functions. It leverages smart contracts for efficiency, ensuring traceability and transparency, promoting connectivity and structured information flows, and emphasizing customer relations management (Czachorowski et al., 2019; Surucu-Balci et al., 2024).

Finally, this framework presents a few functions of Bowtie analysis, there are more functions can be explored. For example, BowTie XP can present the duty of the person who take the responsibility of certain barriers (e.g., “Education and Training” might be held by HR, whereas the responsibility of “up-to-date anti-virus software” would be IT department). Future research can expand the framework and apply more functions (not limited to the abovementioned responsibility and escalation factor) to make the framework comprehensive.

7

CONCLUSIONS AND FURTHER RESEARCH

7.1 Research Contribution

This research holds several significant points:

First, while several studies have addressed maritime risk, safety, and security, research specifically focused on maritime cybersecurity remains limited. To address this gap, this research systematically identifies various cyber threats in the maritime sector and categorises them into groups. This categorisation assists maritime managers in understanding which cyber threats may impact their cybersecurity management and which threats are relatively more critical. This knowledge is especially useful for allocating limited budgets to cybersecurity management in their companies.

Second, in addition to identifying and assessing cyber threats, this research proposes seven risk control measures and six hierarchical criteria for maritime cybersecurity evaluation. This framework helps maritime managers comprehend the importance of these measures and adapt their cybersecurity strategies to different circumstances. For instance, some companies may prioritise the reliability of measures, while others may emphasise economic affordability. The research also suggests various policies for stakeholders to enhance maritime cybersecurity.

Third, this research not only presents a framework for maritime cybersecurity but also conducts risk assessments and evaluates risk control measures using empirical data using industry experts, rather than relying on secondary data. This approach provides real-world insights and reflects the current state of maritime cybersecurity.

Fourth, the research introduces a bowtie framework for maritime cybersecurity risk management, illustrating its use by assessing the risk related to malwares. The visual representation of the bowtie framework aids managers in understanding maritime cyber threats, potential consequences, and risk control measures to mitigate these threats and their consequences.

7.2 Research Limitations

Although the research aim and objectives have been achieved, several research limitations exist in this research. The limitations are highlighted in each corresponding chapter; (please see Section 4.6,5.5, and 6.7). Some more general limitation is presented below.

First, the number of responses could have been higher. For example, the response numbers to Questionnaires 1 and 2 are 31 and 44, respectively; this is probably because the questionnaires (especially Questionnaire 2) are complicated and not easy to be answered, which reduces respondents' willingness to answer the questionnaires. Although the results are tested to be reliable and insightful, a higher number of responses could lead to new perspectives.

Second, in Chapter 4, tangible cybersecurity threats were solely identified through an academic literature review. Nonetheless, considering the multitude of cyberattacks in the marine sector, a more robust identification of cybersecurity threats for future research can be achieved by integrating databases containing real-world cyberattack cases with insights gleaned from academic literature. This approach will enable us to discern which cybersecurity threats are prevalent in actual practice.

Third, threats related to onboard systems are not always the same as those related to office computers; there are also differences in the network design and systems used in administration offices and those, say, in ports. Similarly, the consequences of an attack on a small shipping company are not the same as those of a similar attack on a large company, an international organisation or a governmental office.

Fourth, In Chapter 5, the risk control measure was prioritised using the Fuzzy TOPSIS technique. However, there are potential areas for further investigation regarding the methodology employed. Specifically, the normalisation step and the distance measures utilised in the TOPSIS approach could be explored and extended. Normalisation, which is a crucial aspect of all Multiple Criteria Decision Making (MCDM) methods, could be examined using various approaches such as linear, logarithmic, Markovic, Tzeng, and Huang methods. Conducting such comparisons and evaluating the resulting outcomes could be a valuable direction for future research.

Finally, in Chapter 6, it is important to note that the bowtie analysis approach may not always be suitable for addressing complex situations that require quantitative assessment. This is primarily due to the time-consuming and challenging nature of managing bowtie diagrams, particularly in complex systems that involve multiple hazards. In such cases, it becomes necessary to develop separate diagrams for each identified hazard to accurately capture the complexities involved. Additionally, representing the impact of each threat on the corresponding consequences can pose difficulties within the bowtie framework. Therefore, alternative approaches may need to be considered to effectively address these challenges and provide a more comprehensive representation of the relationship between threats and their associated consequences.

7.3 Suggestions for Further Research

A number of suggestions for future research has been presented in each Chapter; the limitations that were presented in the previous Section could also be addressed in future research. Some more general suggestions are presented below.

Firstly, it is important to acknowledge some onboard IT/OT threats were not included in Questionnaire 2, leading to a potential limitation in the comprehensiveness of the results, particularly in the context of the maritime sector. Despite this, it is crucial to emphasise the assessment of onboard cybersecurity. This aspect holds unique significance within the maritime industry, distinguishing it from other sectors. Therefore, future research should place greater emphasis on the assessment of risks associated with onboard IT/OT systems.

Secondly, exploring variations in opinions among different groups is a promising avenue for research. In our research, younger (and thus less experienced) domain experts might be more cybersecurity aware as younger groups are more familiar with modern IT systems. An interesting finding of our analysis is that junior respondents have a higher mean value in most cyber threat estimates compared to those senior experts. This can be a notable insight for seafarers' training, and company managers should pay more attention to enhancing the cybersecurity awareness of more senior staff. Future research can also address the risk perception of different respondents' backgrounds (e.g., based on their position, department, education, work experience, etc.) through the use of statistics such as t-test or Analysis of variance (ANOVA) models. The finding will provide further justification for the implementation of different control measures with regard to various stakeholder groups.

Third, further development of the bowtie framework is needed. This research provides just an illustration of the framework. Enhancements (such as a risk matrix that addresses various types of consequences) can facilitate a clearer understanding of the risk management process for maritime cybersecurity. Additionally, as the bowtie method combines event tree and fault tree analysis, future research could explore alternative methods, such as fuzzy theory, to address uncertainty in decision-making within the bowtie framework.

Fourthly, the increasing prominence of Maritime Autonomous Surface Ships (MASS) necessitates a heightened focus on their reliance on Information Technology (IT) and

Information and Communication Technology (ICT). This reliance exposes MASS to the risk of cyberattacks by malicious actors. Therefore, conducting further research to identify cyber threats specific to MASS and establishing a cybersecurity risk framework tailored to their needs is of great importance. The maritime cybersecurity framework proposed in this study is relevant to the emerging domain of MASS, which demands comprehensive attention to cybersecurity risk assessment and management.

Lastly, the provision of cybersecurity education to stakeholders within the maritime sector holds significant importance. Our analysis underscores the critical nature of training and education in raising awareness of associated risks. Furthermore, cybersecurity awareness plays a pivotal role in countering the mounting cyber threats faced by maritime vessels, ports, and essential infrastructure. Consequently, in-depth research into the effectiveness of cybersecurity awareness initiatives and crew education in bolstering cybersecurity is crucial for shaping future research efforts.

REFERENCES

Abbassi, R., Khan, F., Khakzad, N., Veitch, B., and Ehlers, S. (2017). Risk analysis of offshore transportation accident in arctic waters. International Journal of Maritime Engineering, 159(A3).

Abdo, H., Kaouk, M., Flaus, J. M., and Masse, F. (2018). A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis. Computers and security, 72, 175-195.

Abeyratne, R. (2016). Aviation Cyber Security: A Constructive Look at the Work of ICAO. Air and Space Law, 41(1).

ABS. (2016). Guidance Note on; The Application of Cybersecurity Priciples to Maritne and Offshore Operations. Available at: http//maritimesafetyinnovationlab.org/wp-content/uploads/2016/09/abs-guidance-on- the-application-of-cyber-security-principles-2016_09.pdf [Accessed: 11th December,2023]

Afenyo, M., and Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. Ocean and Coastal Management, 236, 106493.

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., and Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. Network, 2(1), 123-138.

Akyuz, E., Arslan, O., and Turan, O. (2020). Application of fuzzy logic to fault tree and event tree analysis of the risk for cargo liquefaction on board ship. Applied Ocean Research, 101, 102238.

Alani, S. H. N., and Mahjoob, A. M. R. (2021). Corruption risk analysis at the project planning stage in the Iraqi construction sector using the bowtie methodology. Engineering, Technology and Applied Science Research, 11(3), 7223-7227.

Albery, S., Borys, D., and Tepe, S. (2016). Advantages for risk assessment: Evaluating learnings from question sets inspired by the FRAM and the risk matrix in a manufacturing environment. Safety science, 89, 180-189.

Alcaide, J. I., and Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia, 45, 547-554.

Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., and Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. Sensors, 21(20), 6901.

Alsalem, M. A., Zaidan, A. A., Zaidan, B. B., Hashim, M., Albahri, O. S., Albahri, A. S., and Mohammed, K. I. (2018). Systematic review of an automated multiclass detection and classification system for acute Leukaemia in terms of evaluation and benchmarking, open challenges, issues and methodological aspects. Journal of medical systems, 42, 1-36.

Alyami, H., Yang, Z., Riahi, R., Bonsall, S., and Wang, J. (2019). Advanced uncertainty modelling for container port risk analysis. Accident Analysis and Prevention, 123, 411-421.

Andrews, J. D., and Dunnett, S. J. (2000). Event-tree analysis using binary decision diagrams. IEEE Transactions on Reliability, 49(2), 230-238.

Androjna, A., Brcko, T., Pavic, I., and Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. Journal of Marine Science and Engineering, 8(10), 776.

API. (2016). Process Safety Performance Indicators for the Refining and Petrochemical Industries, API RP 754, 2nd Ed., American Petroleum Institute, Washington DC.

Apostolakis, G. E. (2004). How useful is quantitative risk assessment?. Risk Analysis: An International Journal, 24(3), 515-520.

Aria, M., and Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. Journal of informetrics, 11(4), 959-975.

Arici, S. S., Akyuz, E., and Arslan, O. (2020). Application of fuzzy bow-tie risk analysis to maritime transportation: The case of ship collision during the STS operation. Ocean Engineering, 217, 107960.

Arnetz, J. E., Hamblin, L., Ager, J., Aranyos, D., Upfal, M. J., Luborsky, M., and Essenmacher, L. (2014). Application and implementation of the hazard risk matrix to identify hospital workplaces at risk for violence. American journal of industrial medicine, 57(11), 1276-1284.

ASC Staff. (2017). logisticsmiddleeast.com, Cyberattack on Clarkson's shipbroker reaffirms industry's vulnerability, Available at: https://www.logisticsmiddleeast.com/transport/article-13696-cyberattack-on-clarksons-shipbroker-reaffirms-industrys-vulnerability [Accessed: 11th December,2023]

Ashraf, I., Park, Y., Hur, S., Kim, S.W., Alroobaea, R., Zikria, Y.B. and Nosheen, S. (2022) A survey on cyber security threats in IoT-enabled maritime industry. IEEE Transactions on Intelligent Transportation Systems. 1-14.

Asllani, A., Lari, A., and Lari, N. (2018). Strengthening information technology security through the failure modes and effects analysis approach. International Journal of Quality Innovation, 4(1), 1-14.

Astles, K. L., and Cormier, R. (2018). Implementing sustainably managed fisheries using ecological risk assessment and bowtie analysis. Sustainability, 10(10), 3659.

Aust, J., and Pons, D. (2019). Bowtie methodology for risk analysis of visual borescope inspection during aircraft engine maintenance. Aerospace, 6(10), 110.

Aust, J., and Pons, D. (2020). A systematic methodology for developing bowtie in risk assessment: application to borescope inspection. Aerospace, 7(7), 86.

Aven, T. (2007). A unified framework for risk and vulnerability analysis covering both safety and security. Reliability engineering and System safety, 92(6), 745-754.

Aven, T. (2010). On how to define, understand and describe risk. Reliability Engineering and System Safety, 95(6), 623-631.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253(1), 1-13.

Bai, X., Cheng, L., and Iris, Ç. (2022). Data-driven financial and operational risk management: Empirical evidence from the global tramp shipping industry. Transportation Research Part E: Logistics and Transportation Review, 158, 102617.

Bakioglu, G., and Atahan, A. O. (2021). AHP integrated TOPSIS and VIKOR methods with Pythagorean fuzzy sets to prioritize risks in self-driving vehicles. Applied Soft Computing, 99, 106948.

Balduzzi, M., Pasta, A., and Wilhoit, K. (2014). A security evaluation of AIS automated identification system. In Proceedings of the 30th annual computer security applications conference (pp. 436-445).

Bayazit, O., and Kaptan, M. (2023). Evaluation of the risk of pollution caused by ship operations through bow-tie-based fuzzy Bayesian network. Journal of Cleaner Production, 382, 135386.

BBC News, (2022). European oil facilities hit by cyber-attacks, Available at: https://www.bbc.co.uk/news/technology-60250956. [Accessed: 11th December,2023]

BBC News. (2013). Police warning after drug traffickers' cyber-attack, 2013. Available at: http://www.bbc.corn/news/world-europe-24539417. [Accessed: 11th December,2023]

BBC News. (2018). San Diego port hit by ransomware attack, Available at: https://www.bbc.co.uk/news/technology-45677511. [Accessed: 11th December,2023]

Behzadian, M., Otaghsara, S. K., Yazdani, M., and Ignatius, J. (2012). A state-of the-art survey of TOPSIS applications. Expert Systems with applications, 39(17), 13051-13069.

Bensaci, C., Zennir, Y., Pomorski, D., Innal, F., Liu, Y., and Tolba, C. (2020). STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison. Alexandria Engineering Journal, 59(5), 3799-3816.

Bernsmed, K., Frøystad, C., Meland, P. H., Nesheim, D. A., and Rødseth, Ø. J. (2017). Visualizing cyber security risks with bow-tie diagrams. In International Workshop on Graphical Models for Security (pp. 38-56). Springer, Cham.

BIMCO (2016). The Guidelines on Cyber Security onboard Ships Vol.2

BIMCO (2018). The Guidelines on Cyber Security onboard Ships Vol.3

BIMCO (2020). The Guidelines on Cyber Security onboard Ships Vol.4

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V., and Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. International Journal of Critical Infrastructure Protection, 100571.

Bolbot, V., Theotokatos, G., Boulougouris, E., and Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. Safety Science, 131, 104908.

Bolbot, V., Theotokatos, G., Boulougouris, E., and Vassalos, D. (2019). Safety related cyber-attacks identification and assessment for autonomous inland ships. In International Seminar on Safety and Security of Autonomous Vessels (ISSAV).

Boudehenn, C., Jacq, O., Lannuzel, M., Cexus, J. C., and Boudraa, A. (2021). Navigation anomaly detection: An added value for maritime cyber situational awareness. In 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (pp. 1-4). IEEE.

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., and Lockett-Reynolds, J. (2011). Human performance in cybersecurity: a research agenda. In Proceedings of the Human Factors and Ergonomics Society annual meeting (Vol. 55, No. 1, pp. 1115-1119). Sage CA: Los Angeles, CA: SAGE Publications.

Boyes, H. A. (2014). Maritime cyber security–securing the digital seaways. Engineering and Technology Reference, 1(1), 56-62.

Boyes, H. and Isbell, R. (2017) Code of practice: Cyber security for ships. Institution of Engineering and Technology.

Campisi, T., Marinello, S., Costantini, G., Laghi, L., Mascia, S., Matteucci, F., and Serrau, D. (2022). Locally integrated partnership as a tool to implement a Smart Port

Management Strategy: The case of the port of Ravenna (Italy). Ocean and Coastal Management, 224, 106179.

Canco, I., Kruja, D., and Iancu, T. (2021). AHP, a reliable method for quality decision making: A case study in business. Sustainability, 13(24), 13932.

Canepa, M., Ballini, F., Dalaklis, D. and Vakili, S. (2021) Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain. Proceedings of INTED2021 Conferenceof Conference.

Caponi, S. L., and Belmont, K. B. (2015). Maritime cybersecurity: a growing threat goes unanswered. Intellectual Property and Technology Law Journal, 27(1), 16.

Ceballos, B., Lamata, M. T., and Pelta, D. A. (2017). Fuzzy multicriteria decision-making methods: A comparative analysis. International Journal of Intelligent Systems, 32(7), 722- 738.

Center for Chemical Process Safety. (2018). Bow Ties in Risk Management: A Concept Book for Process Safety. Wiley-AIChE.

Chang, C. H., Kontovas, C., Yu, Q. and Yang, Z. (2021) Risk assessment of the operations of maritime autonomous surface ships. Reliability Engineering and System Safety, 207.

Chang, C. H., Xu, J., and Song, D. P. (2015). Risk analysis for container shipping: from a logistics perspective. The International Journal of Logistics Management.

Chen, C. (2006). CiteSpace II: Detecting and visualizing emerging trends and transient patterns in scientific literature. Journal of the American Society for information Science and Technology, 57(3), 359-377.

Chen, C.T. (2000) Extensions of the TOPSIS for group decision-making under fuzzy environment. Fuzzy Sets and Systems, 114, 1-9.

Chen, P., Zhang, Z., Huang, Y., Dai, L., and Hu, H. (2022). Risk assessment of marine accidents with Fuzzy Bayesian Networks and causal analysis. Ocean and Coastal Management, 228, 106323.

Class NK. (2019). Cyber Security Management Systems for Ships (Requirements and Controls) [First edition]. Class NK, Available at: https://www.classnk.or.jp/hp/en/activities/cybersecurity/csms.html. [Accessed: 11th December,2023]

Corallo, A., Lazoi, M., Lezzi, M. and Luperto, A. (2022) Cybersecurity awareness in the context of the industrial internet of things: A systematic literature review. Computers in Industry, 137, 103614.

Cormier, R., Elliott, M., and Rice, J. (2019). Putting on a bow-tie to sort out who does what and why in the complex arena of marine policy and management. Science of the Total Environment, 648, 293-305.

COSCO World Maritime News, (2018). COSOCO shipping lines falls victim of cyberattack, Available at: https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/ [Accessed: 11th December,2023]

Couce-Vieira, A., Insua, D. R., and Kosgodagan, A. (2020). Assessing and forecasting cybersecurity impacts. Decision Analysis, 17(4), 356-374.

Coventry, L., and Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48-52.

Cox, L. (2008). What's wrong with risk matrices?. Risk Analysis: An International Journal, 28(2), 497-512.

Czachorowski, K., Solesvik, M., and Kondratenko, Y. (2019). The application of blockchain technology in the maritime industry. Green IT engineering: Social, business and industrial applications, 561-577.

Dağdeviren, M., Yavuz, S., and Kılınç, N. (2009). Weapon selection using the AHP and TOPSIS methods under fuzzy environment. Expert systems with applications, 36(4), 8143-8151.

de la Peña Zarzuelo, I., Soeane, M. J. F., and Bermúdez, B. L. (2020). Industry 4.0 in the port and maritime industry: A literature review. Journal of Industrial Information Integration, 20, 100173.

De Peralta, F., Gorton, A., Watson, M., Bays, R., Boles, J., Castleberry, J., and Powers, F. (2020). Framework for Identifying Cybersecurity Vulnerability and Determining Risk for Marine Renewable Energy Systems

de Ruijter, A., and Guldenmund, F. (2016). The bowtie method: A review. Safety science, 88, 211-218.

Dellios, K. and Papanikas, D. (2014) Deploying a maritime cloud. IT Professional, 16 (5), 56-61.

DiRenzo, J., Goward, D. A., and Roberts, F. S. (2015). The little-known challenge of maritime cyber security. In 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA) (pp. 1-5). IEEE.

DNV. (2016). Cyber security resilience management for ships and mobile offshore units in operation 2016 Edition, DNV.

DNV. (2021). Cyber security resilience management for ships and mobile offshore units in operation, 2021 Edition, DNV.

DNV. (2023). The three-pillar approach to cyber security: Data and information protection, DNV, Available at: https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-165683 [Accessed: 8th January,2024]

Drummond, B. M., and Machado, R. C. (2021). Cyber Security Risk Management for Ports-A Systematic Literature Review. In 2021 International Workshop on Metrology for the Sea; Learning to Measure Sea Health Parameters (MetroSea) (pp. 406-411). IEEE.

Eckhart, M., Brenner, B., Ekelhart, A., and Weippl, E. (2019). Quantitative security risk assessment for industrial control systems: Research opportunities and challenges.

Emovon, I., and Aibuedefe, W. O. (2020). Fuzzy TOPSIS application in materials analysis for economic production of cashew juice extractor. Fuzzy Information and Engineering, 12(1), 1-18.

ENISA. (2020). Cyber Risk Management for Ports. Guidelines for cybersecurity in the maritime sector. The European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports. [Accessed: 11th December,2023]

Enoch, S. Y., Lee, J. S., and Kim, D. S. (2021). Novel security models, metrics and security assessment for maritime vessel networks. Computer Networks, 189, 107934.

Ericson, C. A. (2011). System Safety Terms and Concepts. Concise Encyclopedia of System Safety; John Wiley and Sons: Hoboken, NJ, USA, 16-455.

Erstad, E., Lund, M. S., and Ostnes, R. (2022). Navigating through cyber threats, a maritime navigator's experience. Human Factor in Cybersecurity, vol.53, 2022, 84-91, https://doi.org/10.54941/ahfe1002205

Evrin, V. (2021). Risk Assessment and Analysis Methods: Qualitative and Quantitative. ISACA JOURNAL, 28.

Fan, S., Blanco-Davis, E., Yang, Z., Zhang, J., and Yan, X. (2020). Incorporation of human factors into maritime accident analysis using a data-driven Bayesian network. Reliability Engineering and System Safety, 203, 107070.

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

Ferdous, R., Khan, F., Sadiq, R., Amyotte, P. R., and Veitch, B. (2013). Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach.

Process Safety and Environmental Protection, 91(1–2): 1–18. https://doi.org/10.1016/j.psep.2011.08.010

Filinovych, V., and Hu, Z. (2021). Aviation and the Cybersecurity Threats. In International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021) (pp. 120-126). Atlantis Press.

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., Islami, L. and Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. Journal of information security and applications, 61, 102916.

Fitton, O., Prince, D., Germond, B., and Lacy, M. (2015). The future of maritime cyber security.

Fjørtoft, K. E., and Mørkrid, O. E. (2021). Resilience in autonomous shipping. In Proceedings of the 31st European Safety and Reliability Conference. Angers France.

Fouladvand, S., Ghiaci, P., and Shahriari, M. (2010). Fault Tree Analysis, Strengths and Weaknesses. In SHO2010: International Symposium on Occupational Safety and Hygiene (pp. 253-255).

Ghadiminia, N., Mayouf, M., Cox, S., and Krasniewicz, J. (2021). BIM-enabled facilities management (FM): a scrutiny of risks resulting from cyber attacks. Journal of Facilities Management.

Goud. (2019). Cyber Attack on James Fisher and Sons, cybersecurity-insiders, The Wall Street Journal, Available at: https://www.cybersecurity-insiders.com/cyber-attack-on-james-fisher-and-sons/. [Accessed: 11th December,2023]

Goud. (2020). Mediterranean Shipping Company MSC hit by a Cyber Attack, Cybersecurity-insiders, Available at: https://www.cybersecurity-insiders.com/mediterranean-shipping-company-msc-hit-by-a-cyber-attack/. [Accessed: 11th December,2023]

GOV.UK (2022). "Cyber Security Breaches Survey 2022", https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#chapter-5-incidence-and-impact-of-breaches-or-attacks. [Accessed: 11th December,2023]

Guanah, J.S. (2021) Mass media and cyber security in the maritime industry: Analysing the threats and prevention. Global Journal of Arts Humanity and Social Sciences, 2583, 2034.

Gunes, B., Kayisoglu, G., and Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. Computers and Security, 103, 102196.

Gupta, H., and Barua, M. K. (2017). Supplier selection among SMEs on the basis of their green innovation ability using BWM and fuzzy TOPSIS. Journal of Cleaner Production, 152, 242-258

Guzman, N. H. C., Wied, M., Kozine, I., and Lundteigen, M. A. (2020). Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. Systems Engineering, 23(2), 189-210.

Hareide, O. S., Jøsok, Ø., Lund, M. S., Ostnes, R., and Helkala, K. (2018). Enhancing navigator competence by demonstrating maritime cyber security. The Journal of Navigation, 71(5), 1025-1039.

Hasanzadeh, R., Mojaver, P., Azdast, T., Khalilarya, S., Chitsaz, A., and Rosen, M. A. (2023). Decision analysis for plastic waste gasification considering energy, exergy, and environmental criteria using TOPSIS and grey relational analysis. Process Safety and Environmental Protection, 174, 414-423.

Haseeb, J., Mansoori, M., and Welch, I. (2021). Failure Modes and Effects Analysis (FMEA) of Honeypot-Based Cybersecurity Experiment for IoT. In 2021 IEEE 46th Conference on Local Computer Networks (LCN) (pp. 645-648). IEEE.

Hassan, S., Wang, J., Kontovas, C., and Bashir, M. (2022). Modified FMEA hazard identification for cross-country petroleum pipeline using Fuzzy Rule Base and approximate reasoning. Journal of Loss Prevention in the Process Industries, 74, 104616.

Hayes, C. R. (2016). Maritime cybersecurity: the future of national security (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

Heij, C., and Knapp, S. (2018). Predictive power of inspection outcomes for future shipping accidents–an empirical appraisal with special attention for human factor aspects. Maritime Policy and Management, 45(5), 604-621.

Hemminghaus, C., Bauer, J. and Padilla, E. (2021) BRAT: A bridge attack tool for cyber security assessments of maritime systems. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 15.

Hopcraft, R., and Martin, K. M. (2018). Effective maritime cybersecurity regulation–the case for a cyber code. Journal of the Indian Ocean Region, 14(3), 354-366.

Hossain, N. U. I., Nur, F., Hosseini, S., Jaradat, R., Marufuzzaman, M., and Puryear, S. M. (2019). A Bayesian network-based approach for modeling and assessing resilience: A case study of a full service deep water port. Reliability Engineering and System Safety, 189, 378-396.

Hurst, S., and Lewis, S. (2005). Lessons Learned from Real World Application of Bow-Tie Method. United Kingdom: Risktec Solutions Limited, 1.

Hwang, C.-L. and Yoon, K. (1981) Methods for multiple attribute decision making. In: (ed.) Multiple attribute decision making. Springer. pp. 58-191.

Hwang, C.-L., Lai, Y.-J. and Liu, T.-Y. (1993) A new approach for multiple objective decision making. Computers and Operations Research, 20 (8), 889-899.

ICAO. (2016). Resolution A39-19 – Addressing Cybersecurity in Civil Aviation of 2016. the International Civil Aviation Organization. Available at: https://www.icao.int/aviationcybersecurity/Pages/default.aspx [Accessed: 27th December,2023].

ICAO. (2019 a). Aviation Cybersecurity Strategy. International Civil Aviation Organization. Available at: https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx [Accessed: 27th December,2023].

ICAO. (2019 b). Resolution A40-10 – Addressing Cybersecurity in Civil Aviation. Available at: https://www.icao.int/aviationcybersecurity/Pages/default.aspx [Accessed: 27th December,2023].

ICAO. (2022). Resolution A41-19 – Addressing Cybersecurity in Civil Aviation.,. Available at: https://www.icao.int/aviationcybersecurity/Pages/default.aspx [Accessed: 27th December,2023].

IHS Markit. (2016). Cyber security survey in association with BIMCO. Available at: https://cybersail.org/wp-content/uploads/2017/02/IHS-BIMCO-Survey-Findings.pdf.

IHS Markit. (2018). Maritime cyber survey 2018 - the results. Available at: https ://bi-cd02.bimco.org/-/media/bimco/news-and-trends/news/security/cyber-security/2018/fairplay-and-bimco-maritime-cyber-security-survey-2018.ashx. [Accessed: 11th December,2023]

IMO. (2017a.) MSC-FAL.1/Circ.3., Available at: https://www.gard.no/Content/ 23896593/MSC-FAL.1-Circ.3.pdf. [Accessed: 11th December,2023]

IMO. (2017b) MSC 428 (98)., Available at: https://www.imo.org/en/OurWork/ Security/Pages/Cyber-security.aspx. [Accessed: 11th December,2023]

IMO. (2018). Revised Guidelines for Formal Safety Assessment (FSA) For Use in The IMO Rule-Making Process. MSC-MEPC.2/Circ.12/Rev.2. Available at: https://www.imo.org/en/OurWork/Safety/Pages/FormalSafetyAssessment.aspx. [Accessed: 11th December,2023]

IMO. (2021) MSC-FAL.1/Circ.3/Rev.1 Available at: https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf. [Accessed: 11th December,2023]

Imran, Z., and Nizami, R. (2011). Advance secure login. International Journal of Scientific and Research Publications, 1(1), 1-4.

IOGP. (2016). The International Association of Oil Gas Producers. Process Safety – Leading key performance indicators Supplement to Report No. 456. Report No. 556.

IRClass. (2017). Guidelines on Maritime Cyber Safety (IRS-G-SAF-02-2017). The Indian Register of Shipping. Available at: https://www.irclass.org/media/3635/guidelines-on-maritime-cyber-safety_1.pdf. [Accessed: 11th December,2023]

IRClass. (2019). Guidelines on Certification of Software for Computer Based Control Systems' (IRS-G-DES-01—2019). The Indian Register of Shipping. Available at: https://www.irclass.org/media/4155/guidelines-on-certification-of-software-for-computer-based-control-systems_2019.pdf. [Accessed: 11th December,2023]

ISN. (2018). Information Security Newspaper, Hacking attack in port of Barcelona, Available at: https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/. [Accessed: 11th December,2023]

ISO. (2009). Risk management - Principles and guidelines. ISO 31000:2009. Available at: https://www.iso.org/standard/43170.html. [Accessed: 11th December,2023]

ISO. (2018). Risk management - Guideline. ISO 31000:2018. Available at: https://www.iso.org/standard/65694.html. [Accessed: 11th December,2023]

ISO. (2022a). Information security management systems. ISO/IEC 27001:2022. Available at: https://www.iso.org/standard/27001. [Accessed: 11th December,2023]

ISO. (2022b). Guidance on performing risk assessment in the design of onshore LNG installations including the ship/shore interface. ISO/TS 16901:2022. Available at: https://www.iso.org/standard/83773.html. [Accessed: 11th December,2023]

Jang-Jaccard, J. and Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80 (5), 973-993.

Jones, B., Jenkinson, I., Yang, Z., and Wang, J. (2010). The use of Bayesian network modelling for maintenance planning in a manufacturing industry. Reliability Engineering and System Safety, 95(3), 267-277.

Jones, K.D., Tam, K. and Papadaki, M. (2016). Threats and impacts in maritime cyber security. Engineering and Technology Reference, 1 (1).

Kabir, U. Y., Ezekekwu, E., Bhuyan, S. S., Mahmood, A., and Dobalian, A. (2020). Trends and best practices in health care cybersecurity insurance policy. Journal of healthcare risk management, 40(2), 10-14.

Kagalwalla, N., and Churi, P. P. (2019). Cybersecurity in aviation: An intrinsic review. In 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA) (pp. 1-6). IEEE.

Kala, N., and Balakrishnan, M. (2019). Cyber Preparedness in Maritime Industry. International Journal of Scientific and Technical Advancements, 5(2), 19-28.

Kalogeraki, E. M., Apostolou, D., Polemi, N., and Papastergiou, S. (2018a). Knowledge management methodology for identifying threats in maritime/logistics supply chains. Knowledge management research and practice, 16(4), 508-524.

Kalogeraki, E. M., Papastergiou, S., Mouratidis, H., and Polemi, N. (2018b). A novel risk assessment methodology for SCADA maritime logistics environments. Applied Sciences, 8(9), 1477.

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., and Chang, C. H. (2022). Maritime cybersecurity: are onboard systems ready? Maritime Policy and Management, 1-19.

Kaplan, S., and Garrick, B. J. (1981). On the quantitative definition of risk. Risk analysis, 1(1), 11-27.

Kara, E. G. E. (2022). Determination of maritime safety performance of flag states based on the Port State Control inspections using TOPSIS. Marine Policy, 143, 105156.

Karaca, İ., and Söner, Ö. (2023). An Evaluation of Students' cybersecurity Awareness in the Maritime Industry. International Journal of 3D Printing Technologies and Digital Industry, 7(1), 78-89.

Karahalios, H. (2017). The application of the AHP-TOPSIS for evaluating ballast water treatment systems by ship operators. Transportation Research Part D: Transport and Environment, 52, 172-184.

Karahalios, H. (2020). Appraisal of a Ship’s Cybersecurity efficiency: the case of piracy. Journal of Transportation Security, 13(3-4), 179-201.

Karim, M. S. (2020). Australia's engagement in the International Maritime Organisation for Indo-Pacific Maritime Security. Ocean and Coastal Management, 185, 105032.

Karthikeyan, R., Venkatesan, K. G. S., and Chandrasekar, A. (2016). A comparison of strengths and weaknesses for analytical hierarchy process. Journal of Chemical and Pharmaceutical Sciences, 9(3), 12-15.

Kaspersky. (2020). The state of Industrial Cybersecurity in the era of digitalization. Availability at: https://ics.kaspersky.com/media/Kaspersky_ARC_ICS-2020-Trend-Report.pdf

Kavallieratos, G., and Katsikas, S. (2020). Managing cyber security risks of the cyber-enabled ship. Journal of Marine Science and Engineering, 8(10), 768.

Kayisoglu, G., Bolat, P., and Tam, K. (2022). Determining Maritime Cyber Security Dynamics and Development of Maritime Cyber Risk Check List for Ships.

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., and Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. International Journal of Critical Infrastructure Protection, 37, 100526.

Kennedy, G. A. L., Shirvani, F., Scott, W. R., and Campbell, A. P. (2021). Extending model-based approaches to integrate human factors aspects into cybersecurity and safety assessments. In CORE 2021: Collaborating to Master Complexity: Conference on Railway Excellence, 21-23 June 2021, Perth, WA, Australia.

Khan, R. U., Yin, J., Mustafa, F. S., and Anning, N. (2021). Risk assessment for berthing of hazardous cargo vessels using Bayesian networks. Ocean and Coastal Management, 210, 105673.

Khan, S. K., Shiwakoti, N., and Stasinopoulos, P. (2022). A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. Accident Analysis and Prevention, 165, 106515.

King, T., Van Welter, C., and Svensen, T. E. (2016). Stability barrier management for large passenger ships. Ocean Engineering, 125, 342-348.

Kontovas, C. (2011). Quantitative risk management framework for maritime safety and environmental protection (Doctoral dissertation, Εθνικό Μετσόβιο Πολυτεχνείο (ΕΜΠ). Σχολή Ναυπηγών Μηχανολόγων Μηχανικών).

Kontovas, C. A., and Psaraftis, H. N. (2009). CO 2 emission statistics for the world commercial fleet. WMU Journal of Maritime Affairs, 8, 1-25.

Kontovas, C. A., and Psaraftis, H. N. (2010). Carbon dioxide emissions valuation and its uses. In Proc. 3rd International Symposium on Ship Operations, Management and Economics of the Society of Naval Architects Marine Engineers (SNAME) (pp. 7-8).

Kontovas, C. A., and Sooprayen, K. (2020). Maritime Cargo Prioritisation during a Prolonged Pandemic Lockdown Using an Integrated TOPSIS-Knapsack Technique: A Case Study on Small Island Developing States—The Rodrigues Island. Sustainability, 12(19), 7992.

Koola, P.M. (2018). Cybersecurity: A deep dive into the Abyss. Marine Technology Society Journal, 52 (5), 31-43.

Korean Register. (2023). Cyber Risk Management Framework. Available at: https://www.krs.co.kr/eng/Content/CF_View.aspx?MRID=426

Kuhn, K., Bicakci, S., and Shaikh, S. A. (2021). COVID-19 digitization in maritime: understanding cyber risks. WMU Journal of Maritime Affairs, 20(2), 193-214.

Lagouvardou, S. (2018). Maritime Cyber Security: concepts, problems and models. Kongens Lyngby, Copenhagen.

Lee, A. R., and Wogan, H. P. (2018). All at Sea: The Modern Seascape of Cybersecurity Threats of the Maritime Industry. In OCEANS 2018 MTS/IEEE Charleston (pp. 1-8). IEEE.

Lekota, F., and Coetzee, M. (2021). Aviation Sector Computer Security Incident Response Teams: Guidelines and Best Practice. In European Conference on Cyber Warfare and Security (pp. 507-XII). Academic Conferences International Limited.

Li, Z. and Kang, R. (2015) Strategy for reliability testing and evaluation of cyber physical systems. 2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) 6-9 December, Singapore.

Linton Art, Port Authority Role in Cyber-Security, Linked in, (2016). Available at: https://www.linkedin.com/pulse/port-authority-role-cyber-security-art-linton/ [Accessed: 11th December,2023]

Lu, J., Su, W., Jiang, M., and Ji, Y. (2022). Severity prediction and risk assessment for non-traditional safety events in sea lanes based on a random forest approach. Ocean and Coastal Management, 225, 106202.

Lu, L., Liang, W., Zhang, L., Zhang, H., Lu, Z., and Shan, J. (2015). A comprehensive risk evaluation method for natural gas pipelines by combining a risk matrix with a bow-tie model. Journal of Natural Gas Science and Engineering, 25, 124-133.

Luo, T., Wu, C., and Duan, L. (2018). Fishbone diagram and risk matrix analysis method and its application in safety assessment of natural gas spherical tank. Journal of Cleaner Production, 174, 296-304.

Lykou, G., Anagnostopoulou, A., and Gritzalis, D. (2018). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. Sensors, 19(1), 19.

Mahamid, I. (2011). Risk matrix for factors affecting time delay in road construction projects: owners' perspective. Engineering, Construction and Architectural Management.

Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2(2), 109-134.

Manikandan, N., Kumanan, S., and Sathiyanarayanan, C. (2017). Multiple performance optimization of electrochemical drilling of Inconel 625 using Taguchi based Grey Relational Analysis. Engineering Science and Technology, an International Journal, 20(2), 662-671.

Mardani, A., Jusoh, A., Zavadskas, E. K., Cavallaro, F., and Khalifah, Z. (2015). Sustainable and renewable energy: An overview of the application of multiple criteria decision making techniques and approaches. Sustainability, 7(10), 13947-13984.

Matsikidze, H., and Kyobe, M. (2020, November). A Proposed Cyber security framework for auditing in financial institutions. In 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 0276-0281). IEEE.

Mazzarolo, G., and Jurcut, A. D. (2019). Insider threats in Cyber Security: The enemy within the gates. arXiv preprint arXiv:1911.09575.

McLeod, R. W., and Bowie, P. (2018). Bowtie Analysis as a prospective risk assessment technique in primary healthcare. Policy and Practice in Health and Safety, 16(2), 177-193.

Meland, P. H., Bernsmed, K., Frøystad, C., Li, J., and Sindre, G. (2019). An experimental evaluation of bow-tie analysis for security. Information and Computer Security.

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

Mishra, A., Alzoubi, Y. I., Gill, A. Q., and Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. Sensors, 22(2), 538.

Mission secure. (2021). A Comprehensive Guide to Maritime Cybersecurity. Mission secure.com. Available at: https://www.missionsecure.com/resources/comprehensive-guide-to-operational- technology-security-ebook [Accessed: 11th December,2023]

MODU. (2013). Mobile Offshore Drilling Unit. Available at: https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities [Accessed: 11th December,2023]

Mohammadfam, I., Kalatpour, O., and Gholamizadeh, K. (2020). Quantitative assessment of safety and health risks in HAZMAT road transport using a hybrid approach: a case study in Tehran. ACS Chemical Health and Safety, 27(4), 240-250.

Mohd Nizam Ong, N. A. F., Mohd Tohir, M. Z., Mutlak, M. M., Sadiq, M. A., Omar, R., and Md Said, M. S. (2022). BowTie analysis of rooftop grid-connected photovoltaic systems. Process Safety Progress, 41, S106-S117.

Mohr, R. (2016) Evaluating cyber risk in engineering environments: A proposed frame-work and methodology.

Mokhtari, K., Ren, J., Roberts, C., and Wang, J. (2011). Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals. Journal of hazardous materials, 192(2), 465-475.

Morse, E. A., and Raval, V. (2008). PCI DSS: Payment card industry data security standards in context. Computer Law & Security Review, 24(6), 540-554.

Mraković, I., and Vojinović, R. (2019). Maritime cyber security analysis–how to reduce threats? Transactions on maritime science, 8(01), 132-139.

Mullins, B. T., McGurk, R., McLeod, R. W., Lindsay, D., Amos, A., Gu, D., ... and Mazur, L. (2019). Human error Bowtie analysis to enhance patient safety in radiation oncology. Practical Radiation Oncology, 9(6), 465-478.

Munim, Z. H., Dushenko, M., Jimenez, V. J., Shakil, M. H., and Imset, M. (2020). Big data and artificial intelligence in the maritime industry: a bibliometric review and future research directions. Maritime Policy and Management, 47(5), 577-597.

National Cyber Security Centre. (2019). Password policy: updating your approach. https://www.ncsc.gov.uk/collection/passwords/updating-your-approach [Accessed: 11th December,2023]

NIST. (2014). "Framework for Improving Critical Infrastructure Cybersecurity", National Institute of Standards and Technology, Version 1.0. Available at: https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf [Accessed: 23th January,2024]

NIST. (2015). "Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity", National Institute of Standards and Technology, NISTIR 8074 Volume 2. Available at: https://csrc.nist.gov/glossary/term/cybersecurity [Accessed: 11th December,2023]

NIST. (2023). Cybersecurity Framework Components. National Institute of Standards and Technology, Available at: https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components [Accessed: 11th December,2023]

O'Dwyer, R., (2020). IMO latest to fall victim to cyber-attack, Smart maritime network, Available at: https://smartmaritimenetwork.com/2020/10/01/imo- latest-to-fall-victim-to-cyber-attack/ [Accessed: 11th December,2023]

Oguztimur, S. (2011). Why fuzzy analytic hierarchy process approach for transport problems?

Omnitrans. (2020). Matson Reports Cyber Attack, Omnitrans.com,Available at: https://www.omnitrans.com/matson-reports-cyber-attack/ [Accessed: 11th December,2023]

Ostrom, L. T., and Wilhelmsen, C. A. (2019). Qualitative and quantitative research methods used in risk assessment. Risk assessment: Tools, techniques, and their applications, Second Edition, 267-281.

Otto, L. (2020). Global challenges in maritime security. Springer.

Park, C., Kontovas, C., Yang, Z., and Chang, C. H. (2023). A BN driven FMEA approach to assess maritime cybersecurity risks. Ocean and Coastal Management, 235, 106480.

Park, C.K., Chang, C. H., Wenming, S., Wei, Z., and Kontovas, C. A. (2019). Evaluating cybersecurity risks in the maritime industry: a literature review. In Proceedings of the international association of maritime universities (IAMU) conference.

Pascarella, G., Rossi, M., Montella, E., Capasso, A., De Feo, G., Botti, G., and Morabito, A. (2021). Risk analysis in healthcare organizations: Methodological framework and critical variables. Risk Management and Healthcare Policy, 2897-2911.

Peng, D., Hou, X., Li, Y., and Mu, Y. (2019). The difference in development level of marine shellfish industry in 10 major producing countries. Marine Policy, 106, 103516.

Pham, D. V., Halgamuge, M. N., Syed, A., and Mendis, P. (2010). Optimizing windows security features to block malware and hack tools on USB storage devices. In Progress in electromagnetics research symposium.

Ploskas, N., and Papathanasiou, J. (2019). A decision support system for multiple criteria alternative ranking using TOPSIS and VIKOR in fuzzy and nonfuzzy environments. Fuzzy Sets and Systems, 377, 1-30.

Polychronis, K., (2020). Cybersecurity at Sea. In: Otto, L. (ed.) Global Challenges in Maritime Security. p. 243 Springer International Publishing.

Progoulakis, I., Rohmeyer, P., and Nikitakos, N. (2021). Cyber Physical Systems Security for Maritime Assets. Journal of Marine Science and Engineering, 9(12), 1384.

Pseftelis, T. and Chondrokoukis, G. (2021) A Study about the Role of the Human Factor in Maritime Cybersecurity. SPOUDAI-Journal of Economics and Business, 71 (1-2), 55-72.

Pyzynski, M., and Balcerzak, T. (2021). Cybersecurity of the Unmanned Aircraft System (UAS). Journal of Intelligent & Robotic Systems, 102(2), 35.

Qazi, A., Shamayleh, A., El-Sayegh, S., and Formaneck, S. (2021). Prioritizing risks in sustainable construction projects using a risk matrix-based Monte Carlo Simulation approach. Sustainable Cities and Society, 65, 102576.

Qbeitah, M. A., and Aldwairi, M. (2018). Dynamic malware analysis of phishing emails. In 2018 9th International Conference on Information and Communication Systems (ICICS) (pp. 18-24). IEEE.

Rahman, S., Hossain, N. U. I., Govindan, K., Nur, F., and 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

Ratnayake, R. C., and Antosz, K. (2017). Development of a risk matrix and extending the risk-based maintenance analysis with fuzzy logic. Procedia Engineering, 182, 602-610.

Rausand, M. (2013). Risk assessment: theory, methods, and applications (Vol. 115). John Wiley and Sons.

Rausand, M., and Hoyland, A. (2003). System reliability theory: models, statistical methods, and applications (Vol. 396). John Wiley and Sons.

Reason, J. (1990). Human error. Cambridge university press.

Ren, A., Wu, D., Zhang, W., Terpenny, J., and Liu, P. (2017). Cyber security in smart manufacturing: Survey and challenges. In IIE Annual Conference. Proceedings (pp. 716-721). Institute of Industrial and Systems Engineers (IISE).

Ren, J., Jenkinson, I., Wang, J., Xu, D. L., and Yang, J. B. (2008). A methodology to model causal relationships on offshore safety assessment focusing on human and organizational factors. Journal of safety research, 39(1), 87-100.

Reynolds, Z., (2018). safetyatsea.net, Australian defence shipbuilder Austral victim of Iranian cyber-attack, Available at: https://safetyatsea.net/news/news-safety/2018/australian-defence-shipbuilder-austral- victim-of-iranian-cyber-attack/. [Accessed: 11th December,2023]

Rezaei, J. (2016). Best-worst multi-criteria decision-making method: Some properties and a linear model. Omega, 64, 126-130.

Rundle, J., (2019). Coast Guard Details February Cyberattack on Ship, The Wall Street Journal, Available at: https://www.wsj.com/articles/coast-guard-details-february-cyberattack-on-ship-11564133401 [Accessed: 11th December,2023]

Salih, M. M., Zaidan, B. B., Zaidan, A. A., and Ahmed, M. A. (2019). Survey on fuzzy TOPSIS state-of-the-art between 2007 and 2017. Computers and Operations Research, 104, 207-227.

SAMA (2017). Cyber security framework. Saudi Arabian Monetary Authority: Riyadh, Saudi Arabia.

Sarvestani, K., Ahmadi, O., Mortazavi, S. B., and Mahabadi, H. A. (2021). Development of a predictive accident model for dynamic risk assessment of propane storage tanks. Process Safety and Environmental Protection, 148, 1217-1232.

Sèbe, M., Christos, A. K., and Pendleton, L. (2019). A decision-making framework to reduce the risk of collisions between ships and whales. Marine Policy, 109, 103697.

Sen, R. (2016). Cyber and information threats to seaports and ships. Maritime Security, 281-302.

Senarak, C. (2021). Port cybersecurity and threat: A structural model for prevention and policy development. The Asian Journal of Shipping and Logistics, 37(1), 20-36.

SEPA. (2016). Scottish Environment Protection Agency, All easures Necessary Environmental Aspects downloadable from https //www.sepa.org.uk/media/ /d all measures necessary guidance.pdf

Sepehri, A., Vandchali, H. R., Siddiqui, A. W., and Montewka, J. (2022). The impact of shipping 4.0 on controlling shipping accidents: A systematic literature review. Ocean Engineering, 243, 110162.

Shabalala,Z., and Heiberg, T., (2021). REUTERS, Cyber attack disrupts major South African port operations, Available at: https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/ [Accessed: 11th December,2023]

Shead, S. (2021) South Africa port operations halted and workers reportedly put on leave after major cyberattack. CNBC, Available at: https://www.cnbc.com/2021/07/27/transnet-halts-port-operations-in- south-africa-after-major-cyberattack.html

Sheehan, B., Murphy, F., Kia, A. N., and Kiely, R. (2021). A quantitative bow-tie cyber risk classification and assessment framework. Journal of Risk Research, 24(12), 1619-1638.

Sheehan, B., Murphy, F., Kia, A. N., and Kiely, R. (2021). A quantitative bow-tie cyber risk classification and assessment framework. Journal of Risk Research, 24(12), 1619-1638.

Shen, C., and Baker, J., (2021). CMA CGM confirms ransomware attack, Lloyd's List, Available at: https://lloydslist.maritimeintelligence.informa.com/LL11 34044/CMA-CGM-confirms-ransomware-attack. [Accessed: 11th December,2023]

Skorupski, J. (2016). The simulation-fuzzy method of assessing the risk of air traffic accidents using the fuzzy risk matrix. Safety science, 88, 76-87.

Smith, K. J., and Dhillon, G. (2020). Assessing blockchain potential for improving the cybersecurity of financial transactions. Managerial Finance, 46(6), 833-848.

Smolarek, L. (2016). Examples of bow-tie risk analysis at maritime transport. Journal of KONES, 23(3), 489-494.

Sotiralis, P., Louzis, K., and Ventikos, N. P. (2019). The role of ship inspections in maritime accidents: An analysis of risk using the bow-tie approach. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of risk and reliability, 233(1), 58-70.

Stastny, P.,and Stoica, A. M. (2022). Protecting aviation safety against cybersecurity threats. In IOP Conference Series: Materials Science and Engineering, Vol. 1226, No. 1, p. 012025. IOP Publishing.

Subagyo, E., Kholil, K., and Ramli, S. (2021). Risk assessment using bowtie analysis: A case study at gas exploration industry PT XYZ Gresik East Java Indonesia. Process Safety Progress, 40(2), e12190.

Suciu, G., Scheianu, A., Petre, I., Chiva, L., and Bosoc, C. S. (2019). Cybersecurity threats analysis for airports. In New Knowledge in Information Systems and Technologies: Volume 2 (pp. 252-262). Springer International Publishing.

Surucu-Balci, E., Iris, Ç., and Balci, G. (2024). Digital information in maritime supply chains with blockchain and cloud platforms: Supply chain capabilities, barriers, and research opportunities. Technological Forecasting and Social Change, 198, 122978.

Svilicic, B., Kamahara, J., Celic, J., and Bolmsten, J. (2019a). Assessing ship cyber risks: A framework and case study of ECDIS security. WMU Journal of Maritime Affairs, 18, 509-520.

Svilicic, B., Kamahara, J., Rooks, M., and Yano, Y. (2019b). Maritime cyber risk management: An experimental ship assessment. The Journal of Navigation, 72(5), 1108-1120.

Svilicic, B., Kristić, M., Žuškin, S. and Brčić, D. (2020) Paperless ship navigation: cyber security weaknesses. Journal of Transportation Security, 13 (3), 203-214.

Taleb-Berrouane, M., Khan, F., and Hawboldt, K. (2021). Corrosion risk assessment using adaptive bow-tie (ABT) analysis.

Tam, K. and Jones, K.D. (2018) Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. Journal of Cyber Policy, 3 (2), 147-164.

Tam, K., and Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk

Tang, Y., Jing, J., Zhang, Z., and Yang, Y. (2017). A quantitative risk analysis method for the high hazard mechanical system in petroleum and petrochemical industry. Energies, 11(1), 14.

TCAJOB Staff, (2020). Cyberattack hobbles Port of Kennewick, tricitiesbusinessnews.com, Available at: https://www.tricitiesbusinessnews.com/2020/12/port-cyberattack/ [Accessed: 11th December,2023]

The Guardian, (2023). DP World hack: port operator gradually restarting operations around Australia after cyber-attack. Available at: https://www.theguardian.com/australia-news/2023/nov/13/australian-port-operator-

hit-by-cyber-attack-says-cargo-may-be-stranded-for-days [Accessed: 11th December,2023]

The Maritime Executive, (2020a). Carnival Corporation Reports Ransomware Attack Accessed Data, Available at: https://maritime-executive.com/article/carnival-corporation-reports-ransomware-attack-accessed-data [Accessed: 11th December,2023]

The Maritime Executive, (2020b). Hurtigruten Reports Passenger Data Exposed in Cyberattack, Available at: https://maritime-executive.com/article/hurtigruten-reports-passenger-data-exposed-in-cyberattack [Accessed: 11th December,2023]

The Maritime Executive, (2020c). AIDA Cancelled Cruises due to Unspecified IT Outage Available at: https://maritime-executive.com/article/aida-canceled-cruises-due-to-unspecified-it-outage [Accessed: 11th December,2023]

The Maritime Executive, (2021a). Naval Dome: Cyberattacks on OT Systems on the Rise, https://www.maritime- executive.com/article/naval-dome-cyberattacks-on-ot-systems-on-the-rise, last accessed 2021/04/25. [Accessed: 11th December,2023]

The Maritime Executive, (2021b). Cyberattack Hits Multiple Greek Shipping Firms, Available at: https://maritime-executive.com/article/cyberattack-hits-multiple-greek-shipping-firms [Accessed: 11th December,2023]

The Maritime Executive, (2022). Cyberattack Threatens Release of Port of Lisbon Data, Available at: https://maritime-executive.com/article/cyberattack-threatens-release-of-port-of-lisbon-data [Accessed: 11th December,2023]

The North of England P&I Association. (2017). Loss Prevention Briefing: Cyber Risks in Shipping. Available at: https://www.nepia.com/ [Accessed: 11th December,2023]

The North of England P&I Association. (2020). Circular 2021/06: Class War Risks—Renewals 2021/2022. Available at: https://www.nepia.com/ [Accessed: 11th December,2023]

The North of England P&I Association. (2021). Class War Risks-Renewals 2021/2022. Available at: https://www.nepia.com/circulars/class-war-risks-renewals-2021-2022/

The Record. (2023). Ransomware attack on maritime software impacts 1,000 ships. Available at: https://therecord.media/ransomware-attack-on-maritime-software-impacts-1000-ships [Accessed: 11th December,2023]

Tonn, G.L., Kesan, J.P., Zhang, L., and Czajkowski, J. (2019). Cyber Risk and Insurance for Transportation Infrastructure. Transport Policy, 79, 103-114,

Torbari,Y., and Saul,J. (2012). Iran's top cargo shipping line says sanctions damage mounting. REUTERS.com. Available at https://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022 [Accessed: 11th December,2023]

Trbojevic, V. M., and Carr, B. J. (2000). Risk based methodology for safety improvements in ports. Journal of hazardous materials, 71(1-3), 467-480.

Tucci, A. E. (2017). Cyber risks in the marine transportation system. In Cyber-Physical Security (pp. 113-131). Springer, Cham.

Turner, C., Hamilton, W. I., and Ramsden, M. (2017). Bowtie diagrams: A user-friendly risk communication tool. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 231(10), 1088-1097

Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T. E., and Nazir, S. (2022). Cyber security risk assessment in autonomous shipping. Maritime economics and logistics, 24(2), 208-227.

Uddin, M. H., Ali, M. H., and Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Management, 22(4), 239-309.

Uflaz, E., Akyüz, E., Bolat, F., Bolat, P., and Arslan, Ö. (2021). Investigation of the effects of mucilage on maritime operation. J. Black Sea/Mediterranean Environment, 140, 153.

UK HSE. (2013). HID Regulatory Model, Safety Management in Major Hazard Industries. UK Health and Safety Executive.

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... and Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current and future trends. Information, 13(3), 146.

UNCTAD. (2017). Review of Maritime transport 2017. Special Chapter: Maritime transport connectivity. Available at: https://unctad.org/publication/review-maritime-transport-2017 [Accessed: 11th December,2023]

UNCTAD. (2022). Review of maritime transport. United Nations Conference on Trade And Development. Available at: https://unctad.org/publication/review-maritime-transport-2022

Uusitalo, L. (2007). Advantages and challenges of Bayesian networks in environmental modelling. Ecological modelling, 203(3-4), 312-318.

Vaidya, O. S., and Kumar, S. (2006). Analytic hierarchy process: An overview of applications. European Journal of operational research, 169(1), 1-29.

Van Eck, N., and Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. scientometrics, 84(2), 523-538.

Vanem, E. (2012). Ethics and fundamental principles of risk acceptance criteria. Safety science, 50(4), 958-967.

Voicu, I., Panaitescu, F. V., Panaitescu, M., Dumitrescu, L. G., and Turof, M. (2018). Risk management with Bowtie diagrams. In IOP Conference Series: Materials Science and Engineering (Vol. 400, No. 8, p. 082021). IOP Publishing.

Volz, D., (2019). The Wall Street Journal, Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets, Available at: https://www.wsj.com/articles/chinese-hackers-target- universities-in-pursuit-of-maritime-military-secrets- 11551781800 [Accessed: 11th December,2023]

Von Solms, R., and Van Niekerk, J. (2013). From information security to cyber security. computers and security, 38, 97-102.

Vu, L., Nguyen, L., Abdelaal, M., Vu, T., and Mohammed, O. (2023). A Cyber-HIL for Investigating Control Systems in Ship Cyber Physical Systems. arXiv preprint arXiv:2306.14017.

Wan, C., Tao, J., Yang, Z., and Zhang, D. (2022). Evaluating recovery strategies for the disruptions in liner shipping networks: a resilience approach. The International Journal of Logistics Management, 33(2), 389-409.

Wan, C., Yan, X., Zhang, D., and Yang, Z. (2019b). Analysis of risk factors influencing the safety of maritime container supply chains. International Journal of Shipping and Transport Logistics, 11(6), 476-507.

Wan, C., Yan, X., Zhang, D., Qu, Z., and Yang, Z. (2019a). An advanced fuzzy Bayesian-based FMEA approach for assessing maritime supply chain risks. Transportation Research Part E: Logistics and Transportation Review, 125, 222-240.

Wang, Y. (2018). Application of TOPSIS and AHP in the multi-objective decision-making problems. In MATEC Web of Conferences (Vol. 228, p. 05002). EDP Sciences.

Wang,Y., Chen, P., Wu,B., Wan,C., and Yang, Z. (2022) A trustable architecture over blockchain to facilitate maritime administration for MASS systems. Reliability Engineering and System Safety, 219, 108246

Wimpenny, G., Šafář, J., Grant, A. and Bransby, M. (2021) Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility. The Journal of Navigation, 1-13.

Yan, X.P., Wan, C.P., Zhang, D. and Yang, Z. (2017) Safety management of waterway congestions under dynamic risk conditions—A case study of the Yangtze River. Applied Soft Computing, 59, 115-128.

Yang, C. C., and Hsu, W. L. (2018). Evaluating the impact of security management practices on resilience capability in maritime firms—A relational perspective. Transportation Research Part A: Policy and Practice, 110, 220-233.

Yang, S. H., Cao, Y., Wang, Y., Zhou, C., Yue, L., and Zhang, Y. (2021). Harmonizing safety and security risk analysis and prevention in cyber-physical systems. Process safety and environmental protection, 148, 1279-1291.

Yang, Y. C. (2011). Risk management of Taiwan's maritime supply chain security. Safety science, 49(3), 382-393.

Yang, Z. L., and Qu, Z. (2016). Quantitative maritime security assessment: a 2020 vision. IMA Journal of Management mathematics, 27(4), 453-470.

Yang, Z. L., Wang, J., and Li, K. X. (2013). Maritime safety analysis in retrospect. Maritime Policy and Management, 40(3), 261-277.

Yang, Z., Bonsall, S. and Wang, J. (2008) Fuzzy rule-based Bayesian reasoning approach for prioritization of failures in FMEA. IEEE Transactions on Reliability, 57 (3), 517-528.

Yang, Z., Ng, A. K., and Wang, J. (2014). A new risk quantification approach in port facility security assessment. Transportation research part A: policy and practice, 59, 72-90.

Yeboah-Boateng, E. O., and Amanor, P. M. (2014). Phishing, SMiShing and Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5(4), 297-307.

Yoo, Y. and Park, H.-S. (2021) Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. Journal of Marine Science and Engineering, 9 (6), 565.

Yoo, Y., and Park, H. S. (2021). Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. Journal of Marine Science and Engineering, 9(6), 565.

Yu, Q., Liu, K., Chang, C. H., and Yang, Z. (2020). Realising advanced risk assessment of vessel traffic flows near offshore wind farms. Reliability Engineering and System Safety, 203, 107086.

Żebrowski, P., Couce-Vieira, A., and Mancuso, A. (2022). A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber-Physical Systems. Risk Analysis, 42(10), 2275-2290.

Zhou, Y., Li, X., and Yuen, K. F. (2022). Holistic risk assessment of container shipping service based on Bayesian Network Modelling. Reliability Engineering and System Safety, 220, 108305.

APPENDIX A – QUESTIONNAIRE 1

Dear Participant,

We are research staff from Liverpool Logistics, Offshore and Marine Research Institute (LOOM) in Liverpool John Moores University. We are currently conducting a research project entitled "Cybersecurity in the maritime industry" funded by the International Association of Maritime Universities (IAMU). The research aim is to investigate the important threats influencing the maritime cybersecurity from different stakeholders' perspectives, including carriers, port authorities, and academia. In order to achieve the research aim, this interview is to obtain an understanding of the perceptions of maritime experts on the possible threats relating to the maritime cybersecurity. Your rich experience in the maritime industry makes your opinion extremely valuable to our research.

Kindly be informed that all answers and information gathered will be treated with the utmost confidentiality and under no circumstances will any of the data be revealed to third parties.

This questionnaire will take you 10 to 15 minutes. Thank you.

If you are interested in participating in the study, please take time to read the participant information sheet and contact me with any questions. We can be contacted by email: c.chang@ljmu.ac.uk; C.Park@2019.ljmu.ac.uk

Best regards,

Dr Chia-Hsun Chang
Dr Wei Zhang
Dr Wenming Shi
Chang-Ki Park

1. There is a list of threats of maritime cybersecurity identified from the literature review, can you please confirm whether they are appropriate (if not, please type "X" in the Rate column) and if there are any more threats that are not identified in the list (please type in the row of Other (please specify))?

   In addition, can you also please rate the risk level of these threats (1: very low risk to 5: very high risk)?

Phishing	
	Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.)
	Downloading attached files from impersonation emails (e.g., bank, credit card company, insurance company, etc.)
	Accessing links from impersonation text massage (e.g., bank, credit card company, insurance company, etc.)
	Other (please specify):
Malware	
	Downloading files (e.g., mp3, movie, games) from suspicious websites
	Accessing links from suspicious emails
	Downloading attached files from unknown emails
	Connecting USB or removable media to computer without virus check
	Accessing malicious advertising on websites
	Other (please specify):
Man in the middle attack	
	Using unsecured open Wi-Fi connection
	Using insecure Virtual Private Network (VPN)
	Applying weak WEP/WPA encryption on access points
	Providing personal/commercial information to friends/partners via an open Wi-Fi connection
	Providing personal/commercial information to suspicious websites (e.g., illegal software/music/movie download websites)
	Other (please specify):
Ransomware	
	Accessing suspicious websites
	Downloading files from P2P site (e.g., torrent files, music, movies, etc.)
	Downloading program from suspicious websites (e.g., illegal software/music/movie download websites)
	Controlled computer by attacker through remote desktop protocol (RDP)
	Connecting your infected USB or removable media to connect computers/navigation systems
	Other (please specify):

Theft of credentials	
	Using automatically log in system (e.g., save your ID and password on website)
	Using simple and easy to assume password
	Applying only single factor authentication for log in account system
	Providing personal information to a fake website (e.g., government website, etc.)
	Other (please specify):
Distributed Denial of Service (DDoS/DoS)	
	DDoS attacks AIS database
	DDoS attacks GPS and RADAR system
	DDoS attacks company's server system
	Other (please specify):
Human error	
	Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it)
	Company does not set a proper cybersecurity process
	Employees do not follow company's cybersecurity process due to poor cybersecurity awareness
	Closing firewall due to careless operations or specific purpose
	Accessing suspicious links due to careless operations or specific purpose
	Other (please specify):
Using outdated IT system	
	Using outdated version firewall and antivirus software
	Using unpatched operating system e.g., outdated window version
	Forgetting update software
	No planning applying up-to-date software
	Other (please specify):

2. What type of your organisation do you work for
   Shipping company
   Port authority
   Government organisation
   University
   Other (please specify):

3. How many years you have been worked in your company/university/organisation?

   _____years.

The questionnaire ends here. Thank you for your participation

APPENDIX B – QUESTIONNAIRE 2

Dear Participant,

We are researchers from Liverpool Logistics, Offshore and Marine Research Institute (LOOM) in Liverpool John Moores University. We are currently conducting a research project entitled "Cybersecurity in the maritime industry" funded by the International Association of Maritime Universities (IAMU). The research aim is to investigate the important threats influencing the maritime cybersecurity from different stakeholders' perspectives, including carriers, port authorities, and academia. In order to achieve the research aim, this interview is to obtain an understanding of the perceptions of maritime experts on the possible threats relating to the maritime cybersecurity. Kindly be informed that all answers and information gathered will be treated with the utmost confidentiality and under no circumstances will any of the data be revealed to third parties. This questionnaire has been approved by LJMU's Research Ethics Committee. This questionnaire will take you around 20 minutes. Thank you.

If you are interested in participating in the study, please take time to read the participant information sheet (attached) and contact us with any questions.

Best regards,

Dr Chia-Hsun Chang (c.chang@ljmu.ac.uk)
Dr Wei Zhang (Vera.zhang@utas.edu.au)
Dr Wenming Shi (Wenming.Shi@utas.edu.au)
Chang-Ki Park (C.Park@2019.ljmu.ac.uk)

Example: To evaluate the risk of illness in winter.

Event	Likelihood					Consequence				
	VL	L	A	H	VH	VL	L	A	H	VH
How likely to eat ice cream during in winter	85%	15%	0%	0%	0%	0%	40%	50%	10%	0%

The explanation of the above example: the likelihood of eating ice cream during winter is 15% Low and 85% Very Low; whereas the consequences is 10% High, 50% Medium, and 40% Low.

The total assessment for each attribute must be equal 100%.

Likelihood of failure	Meaning
Very Low (VL)	Failure is unlikely but possible during lifetime
Low (L)	Likely to happen once a year
Average (A)	Occasional failure (once per quarter)
High (H)	Repeated failure (once per month)
Very High (H)	Failure is almost inevitable or likely to happen repeatedly

Consequence severity	Meaning
Negligible (N)	At most a single minor incident or unscheduled maintenance required
Marginal (MA)	Minor system damage. Operations interrupted slightly and resumed to its usual operational mode within a short period of time. (say less than 6 hours)
Moderate (MO)	Moderate system damage. Operations and production interrupted marginally, and resumed to its usual operational mode within, say no more than 12 hours.
Critical (CR)	Major system damage. Operations stopped. High degree of operational interruption.
Catastrophic (CA)	Total system loss. Very high severity ranking when a potential failure mode affects sailing operations and/or involves non-compliance with government regulations

Probability of the failure being undetected	Meaning
Highly unlikely (HU)	Possible to detect without checks or maintenance
Unlikely (U)	Possible to detect through regular checks or maintenance
Average (A)	Possible to detect through intensive checks or maintenance
Likely (L)	Difficult to detect through intensive or regular checks or maintenance
Highly likely (HL)	Impossible to detect even through intensive or regular checks or maintenance

Part 1: There is a list of threats of maritime cybersecurity identified from the literature review and expert interview, can you please rate the three parameters of these threats (where Likelihood: likelihood of failure, Consequence: consequence severity, Probability: probability of the failure being undetected)?

Threats of maritime cybersecurity															
Phishing	Likelihood (%)					Consequence (%)					Probability (%)				
	VL	L	A	H	VH	N	MA	MO	CR	CA	HU	U	A	L	HL
Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.)															
Downloading attached files from impersonation emails (e.g., bank, credit card company, insurance company, etc.)															
Malware	Likelihood (%)					Consequence (%)					Probability (%)				
	VL	L	A	H	VH	N	MA	MO	CR	CA	HU	U	A	L	HL
Accessing links from suspicious emails															
Downloading attached files from unknown emails															
Connecting USB or removable media to computer without virus check															
Man in the middle attack	Likelihood (%)					Consequence (%)					Probability (%)				
	VL	L	A	H	VH	N	MA	MO	CR	CA	HU	U	A	L	HL
Providing personal/commercial information to friends/partners via open Wi-Fi connection															

Providing personal/commercial information to suspicious websites (e.g., illegal software/music/movie download websites)															
Ransomware	Likelihood (%)					Consequence (%)					Probability (%)				
	VL	L	A	H	VH	N	MA	MO	CR	CA	HU	U	A	L	HL
Accessing suspicious websites															
Connecting your infected USB or removable media to connect computers/navigation systems															
Theft of credentials	Likelihood (%)					Consequence (%)					Probability (%)				
	VL	L	A	H	VH	N	MA	MO	CR	CA	HU	U	A	L	HL
Using automatically log in system (e.g., save your ID and password on website)															
Using simple and easy to assume password															
Applying only single factor authentication for log in account system															
Providing personal information to a fake website (e.g., government website, etc.)															
Distributed Denial of Service (DDoS/DoS)	Likelihood (%)					Consequence (%)					Probability (%)				
	VL	L	A	H	VH	N	MA	MO	CR	CA	HU	U	A	L	HL
DDoS attacks company's server system															
Human Factor	Likelihood (%)					Consequence (%)					Probability (%)				
	VL	L	A	H	VH	N	MA	MO	CR	CA	HU	U	A	L	HL
Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it)															
Company does not set a proper cybersecurity process															
Employees do not follow company's cybersecurity process due to poor cybersecurity awareness															

Closing firewall due to careless operations or specific purpose															
Accessing suspicious links due to careless operations or specific purpose															
Using outdated IT system	Likelihood (%)					Consequence (%)					Probability (%)				
	VL	L	A	H	VH	N	MA	MO	CR	CA	HU	U	A	L	HL
Using outdated version firewall and anti-virus software															
Using unpatched operating system e.g., outdated window version															
Forgetting update software															

Part 2 The following questions will be related to your personal information:

(1) Your work experience in the maritime area:

☐ Less than 5 years ☐ 6 to 10 years ☐ 11 to 15 years ☐ More than 16 years

(2) Your company/organisation:

☐ Shipping company ☐ IMO ☐ Port company ☐ University ☐ Other:_____

The questionnaire ends here. Thank you for your participant.

APPENDIX C – QUESTIONNAIRE 3

Cybersecurity in the maritime industry - Assessment of measures to reduce cybersecurity risk

Dear participants:

My name is Changki Park; I am a PhD student at the Liverpool Logistics, Offshore and Marine Research Institute (LOOM) in Liverpool John Moores University.

Currently, I am doing a research project on "Cybersecurity risk assessment in the maritime industry". The purpose of this questionnaire is to assess strategies of mitigating the cyberattack risk in the maritime sector.

The survey will take approximately 5 minutes of your time. Your participation in this survey is completely voluntary. Kindly be informed that all answers and information gathered will be treated with the utmost confidentiality and under no circumstances will any of the data be revealed to third parties. This questionnaire has been approved by LJMU's Research Ethics Committee (ref: 21/MME/008). There are no risks associated with the study, but if you have any questions regarding the questionnaire or problems answering any questions, please advise or contact the researcher. If you know of others that might be interested in this study, could you please also pass this questionnaire onto them so they may contact the researcher to volunteer for the study? If you have any questions about the study, please do not hesitate to contact me.

Thank you in advance for your help and please do not hesitate to contact me in the email below should you want any further information of clarifications.

Your Sincerely,

Researcher: Park, Chang-Ki

E-mail: C.Park@2019.ljmu.ac.uk

Supervisors: Dr Chang, Chia-Hsun, Dr Kontovas, Christos, Prof Yang, Zaili

PhD. Researcher in Liverpool Logistics, Offshore and Marine (LOOM) Research Institute, Liverpool John Moores University, L3 3AF, United Kingdom.

1. Company/Organisation

   Mark only One Oval

   - ◯ Ship owner/operator Port
   - ◯ operator
   - ◯ Port authority
   - ◯ Regulator (national or international e.g., IMO) Seafarer
   - ◯ Academia
   - ◯ Other pls specify below

2. Company/Organisation (Pls specify if Other)

3. Work experience in maritime area

   Mark only one oval

   - ◯ Less than 5 years
   - ◯ 6-10 years
   - ◯

10-15 years

More than 15 years

4. Locations

Mark only one oval

United Kingdom

Taiwan

Korea

Greece

Other

5. Location (Pls specify if other)

Criteria

Cyber-attacks are defined as an attempt by hackers to damage or destroy a computer network or system. In selecting the best mitigation strategy to reduce the cyberattack risk, please assess the importance of the following criteria. The scale ranges from Very Low to Very High.

The description of the various criteria

Related to the previous question. Please assess the importance of each criterion, from Very low to Very High

*Note this is not a pairwise conversion - PLEASE SELECT ONLY ONE VALUE per criterion/row

MAIN CRITERIA

-- RELIABILITY: it refers to the capability of the interested system to perform as designed, also under particular conditions, and to the durability of the system in case of its failure. In your selection if for example reliability is in your opinion very important in selecting the mitigation strategy then please select very high (VH).

---ECONOMIC AFFORDABILITY: Refers to the economic cost of the proposed mitigation strategy. For example, if you think that the being affordable (i.e. not costing a lot of money) is very important in the decision please select Very High. If you think affordability is not important (e.g the economic cost is not important in the decision) please select Very Low (VL).

-- EASY TO USE: it refers to how straightforward and simple to use/implement the strategy is. This is the non-monetary cost part, for example an easy strategy is one that doesn't require much training, is easy to be implemented etc.

-- Effectiveness in reducing the LIKELIHOOD of a cyberattack: It refers to how important the effectiveness in reducing this risk aspect is.

-- Effectiveness in reducing the SEVERITY of a cyberattack: It refers to how important the effectiveness in reducing this risk aspect (potential or actual consequences/impact) is

-- Effectiveness in reducing the UNDETECTABILITY of a cyberattack: It refers to how important the effectiveness in reducing this risk aspect is. This is related to the likelihood that the cyber-attack is undetected during normal operations before significant cyber-risk attack effects occur.

6. How important are the criteria below for the selection of the best alternative (strategy) to address the risk of cyber-attack? (PLEASE select only one value per row/criterion)

Mark only one oval per row

	Very low	Low	Medium low	Medium	Medium high	High	Very high
RELIABILITY	○	○	○	○	○	○	○
ECONOMIC AFFORDABILITY	○	○	○	○	○	○	○
EASY TO USE	○	○	○	○	○	○	○
Effectiveness in reducing the LIKELIHOOD of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the SEVERITY of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the UNDETECTABILITY of a cyberattack	○	○	○	○	○	○	○

Rate the alternatives (strategies) based on the above criteria

In this last section, we are asking your opinion on the alternatives with respect to various criteria through linguistic terms.

A brief explanation of each alternative is provided below

Education and Training

BIMCO (2018) stated that maritime industry has lack cyber awareness culture and governance in their system and could result in more source of vulnerabilities and thus cause more cyberattack incidents.

One option to address the issue is therefore by education for new staff and regular training for all personnel.

Effective Anti-virus software management

This is related to the use of anti-virus-software including its regular update/maintenance.

Hardware and software maintenance

This is related to regularly updating the existing onboard security and safety systems.

Strong password policy

This is related to enforcing a strong password policy, thus requiring used to use complicated passwords and changing them regularly.

Management of network devices

This is related to the network devices such as servers, routers etc., and their proper set-up and maintenance.

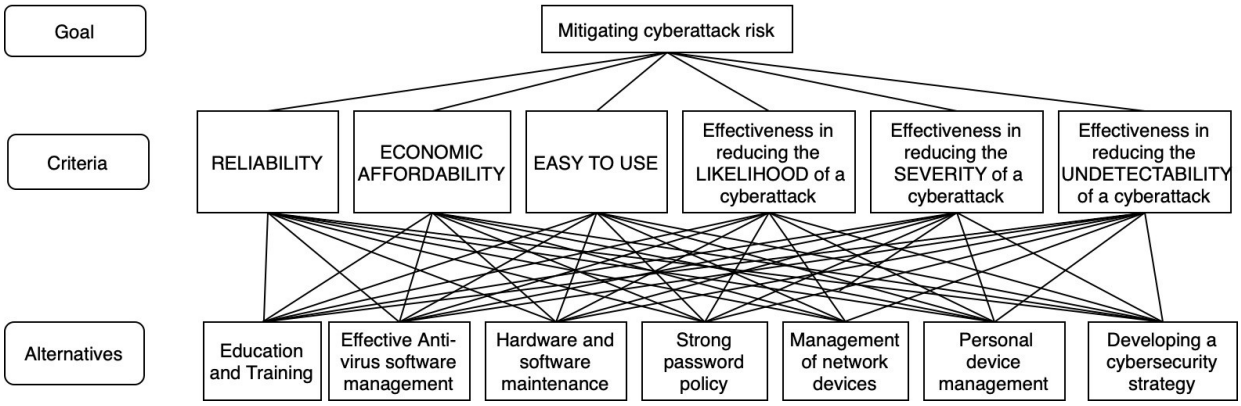
Personal device management

Personal devices such as laptop, smart phone, USB drive are seen as vulnerabilities as they can be used install malicious programmes which can, for example, disrupt systems or steal valuable data/information.

Developing a cybersecurity strategy

Several guidelines recommend setting up cybersecurity strategy which outlines the way to handle events when cybersecurity incidents happen. For example, the IMO Guidelines recommends developing and implement a cyber incident response plan based on a risk assessment.

Criteria and Alternative (strategies) related to the mitigation cyber-attacks



7. Rate the alternatives with respect to RELIABILITY (limited to one response per row). Scale from Very poor reliability to Very good (e.g., highly reliable).

   Mark only one oval per row

	Very low	Low	Medium low	Medium	Medium high	High	Very high
RELIABILITY	○	○	○	○	○	○	○
ECONOMIC AFFORDABILITY	○	○	○	○	○	○	○
EASY TO USE	○	○	○	○	○	○	○
Effectiveness in reducing the LIKELIHOOD of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the SEVERITY of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the UNDETECTABILITY of a cyberattack	○	○	○	○	○	○	○

8. Rate the alternatives with respect to ECONOMIC AFFORDABLITY (limited to one response per row). Scale from Very poor (e.g., Affordable i.e., Very expensive) to Very good (e.g., Very inexpensive)

   Mark only one oval per row

	Very low	Low	Medium low	Medium	Medium high	High	Very high
RELIABILITY	○	○	○	○	○	○	○
ECONOMIC AFFORDABILITY	○	○	○	○	○	○	○
EASY TO USE	○	○	○	○	○	○	○
Effectiveness in reducing the LIKELIHOOD of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the SEVERITY of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the UNDETECTABILITY of a cyberattack	○	○	○	○	○	○	○

9. Rate the alternatives with respect to EASY-TO-USE (limited to one response per row). Scale from Very poor (e.g., NOT easy to use) to Very good (e.g., very easy and straightforward to use/implement).

Mark only one oval per row

	Very low	Low	Medium low	Medium	Medium high	High	Very high
RELIABILITY	○	○	○	○	○	○	○
ECONOMIC AFFORDABILITY	○	○	○	○	○	○	○
EASY TO USE	○	○	○	○	○	○	○
Effectiveness in reducing the LIKELIHOOD of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the SEVERITY of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the UNDETECTABILITY of a cyberattack	○	○	○	○	○	○	○

10. Rate the alternatives with respect to "Effectiveness in Reducing the LIKELIHOOD of Cyber-attack (limited to one response per row). Scale from Very poor (e.g., Very low effect in reducing the likelihood) to Very good (e.g., very good/ effective in reducing the likelihood).

Mark only one oval per row

	Very low	Low	Medium low	Medium	Medium high	High	Very high
RELIABILITY	○	○	○	○	○	○	○
ECONOMIC AFFORDABILITY	○	○	○	○	○	○	○
EASY TO USE	○	○	○	○	○	○	○
Effectiveness in reducing the LIKELIHOOD of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the SEVERITY of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the UNDETECTABILITY of a cyberattack	○	○	○	○	○	○	○

11. Rate the alternatives with respect to "Effectiveness in Reducing the SEVERITY (CONSEQUENCE/IMPACT) of Cyber-attack (limited to one response per row). Scale from Very poor (e.g., Very low effect in reducing the consequences/impact) to Very good (e.g., very good/ effective in reducing the consequences).

Mark only one oval per row

	Very low	Low	Medium low	Medium	Medium high	High	Very high
RELIABILITY	○	○	○	○	○	○	○
ECONOMIC AFFORDABILITY	○	○	○	○	○	○	○
EASY TO USE	○	○	○	○	○	○	○
Effectiveness in reducing the LIKELIHOOD of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the SEVERITY of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the UNDETECTABILITY of a cyberattack	○	○	○	○	○	○	○

12. Rate the alternatives with respect to “Reducing the UNDETECTABILITY i.e., Probability of Cyber-attack being undetected (limited to one response per row). Scale from Very poor (e.g., Very low effect in reducing the probability of cyber-attack being undetected) to Very good (e.g., very good/ effective in reducing the consequences).

Mark only one oval per row

	Very low	Low	Medium low	Medium	Medium high	High	Very high
RELIABILITY	○	○	○	○	○	○	○
ECONOMIC AFFORDABILITY	○	○	○	○	○	○	○
EASY TO USE	○	○	○	○	○	○	○
Effectiveness in reducing the LIKELIHOOD of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the SEVERITY of a cyberattack	○	○	○	○	○	○	○
Effectiveness in reducing the UNDETECTABILITY of a cyberattack	○	○	○	○	○	○	○

APPENDIX D – PUBLICATIONS

Parts of this thesis are based on published material as shown below. Permission has been given by the co-authors to reproduce the relevant material.

Chapter 1 draws some portions from:

1. Park, C.K., Chang, C. H., Wenming, S., Wei, Z., and Kontovas, C. A. (2019). Evaluating cybersecurity risks in the maritime industry: a literature review. Proceedings of the International Association of Maritime Universities (IAMU) Conference, Tokyo, Japan, Nov. 2019, ISSN: 2706-6762.

Chapter 3 is based mainly on material from:

1. Chang, C-H; Zhang, Wei; Shi, Wenming; Park, C (2020). Evaluating cybersecurity in the maritime industry. University Of Tasmania. Conference contribution. https://hdl.handle.net/102.100.100/23100653.v1).

2 Park, C., Kontovas C., Yang Z. and C.-H. Chang. “A BN driven FMEA approach to assess maritime cybersecurity risks”, Ocean and Coastal Management (I.F.: 4.295), 106480, doi:10.1016/j.ocecoaman.2023.106480