

IAMU 2019 Research Project
(No. YAS201902)

**Evaluating cybersecurity in the
maritime industry**

By

Liverpool John Moores University (LJMU)

August 2020

IAMU
International Association of Maritime Universities

International Association of Maritime Universities

This report is published as part of the 2019 Research Project in the 2019 Capacity Building Project of International Association of Maritime Universities, which is fully supported by The Nippon Foundation.

The text of the paper in this volume was set by the author. Only minor corrections to the text pertaining to style and/or formatting may have been carried out by the editors.

All rights reserved. Due attention is requested to copyright in terms of copying, and please inform us in advance whenever you plan to reproduce the same.

The text of the paper in this volume may be used for research, teaching and private study purposes.

No responsibility is assumed by the Publisher, the Editor and Author for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in this book.

Editorial

IAMU Academic Affairs Committee (AAC)

Head of Committee : Professor Dr. Janusz Zarebski

Rector, Gdynia Maritime University (GMU)

Professor Dr. Adam Weintrit

Rector, Gdynia Maritime University (GMU) from 1st Sept. 2020

Editorial committee : Bogumil Laczynski (GMU)

Avtandil Gegenava (BSMA)

Christian Matthews (LJMU)

Contractor : Ahmed Al-Shamma

Research Coordinator: Chia-Hsun Chang

Published by the International Association of Maritime Universities (IAMU) Secretariat

Meiwa Building 8F, 1-15-10 Toranomon, Minato-ku,

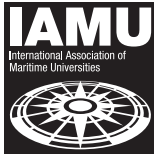
Tokyo 105-0001, JAPAN

TEL : 81-3-6257-1812 E-mail : info@iamu-edu.org URL : <http://www.iamu-edu.org>

Copyright ©IAMU 2020

All rights reserved

ISBN978-4-907408-35-0



IAMU 2019 Research Project
(No. YAS201902)

**Evaluating cybersecurity in the
maritime industry**

By
Liverpool John Moores University

Contractor : Ahmed Al-Shamma
Research Coordinator : Chia-Hsun Chang
Research Partner : Wei Zhang, AMC
Wenming Shi, AMC
Changki Park, LJMU

International Association of Maritime Universities

Contents

| | |
|---|----|
| Executive summary | 2 |
| 1. Introduction | 4 |
| 1.1 Background | 4 |
| 1.2 Research aim and objectives | 4 |
| 1.3 Significance of this research | 4 |
| 1.4 Report structure | 5 |
| 2. Literature review | 5 |
| 2.1 Definition of Cybersecurity | 5 |
| 2.2 Maritime cyberattack incidents | 5 |
| 2.3 Cybersecurity threats in the maritime industry | 7 |
| 2.3.1 Human error | 7 |
| 2.3.2 Using outdated IT system | 7 |
| 2.3.3 Malware | 7 |
| 2.3.4 Phishing | 7 |
| 2.3.5 Man in the middle attack | 7 |
| 2.3.6 Ransomware | 8 |
| 2.3.7 Theft of credentials | 8 |
| 2.3.8 Distribute Denial of Service (DDoS) | 8 |
| 2.4 Risk control options for maritime cybersecurity | 8 |
| 2.4.1 Cybersecurity education and training | 9 |
| 2.4.2 Malware protection software installation | 10 |
| 2.4.3 Software update | 10 |
| 2.4.4 Password policy | 10 |
| 2.4.5 Developing cybersecurity process | 10 |
| 2.4.6 Enhancing cybersecurity awareness | 11 |
| 2.4.7 Firewall, web and mail content filtering and proxy server | 12 |
| 2.5 Cybersecurity barrier management | 12 |
| 3. Methodology | 16 |
| 3.1 Data collection | 16 |
| 3.2 Data analysis method | 17 |

| | | |
|--------|---|----|
| 3.2.1 | Failure Modes and Effects Analysis (FMEA) | 17 |
| 3.2.2 | Rule-based Bayesian networks (RBN)..... | 18 |
| 3.2.3 | Three-dimensional risk matrix | 21 |
| 4. | Research findings..... | 23 |
| 4.1 | Research findings on the first run questionnaire..... | 23 |
| 4.2 | Research findings on Rule-based Bayesian Network | 24 |
| 4.2.1 | Respondents' background..... | 24 |
| 4.2.2 | Research findings on the assessment of the 'Phishing' threat category | 25 |
| 4.2.3 | Research findings on the assessment of the 'Malware' threat category | 26 |
| 4.2.4 | Research findings on the assessment of the 'Man-in-the-middle' threat category | 28 |
| 4.2.5 | Research findings on the assessment of the 'Ransomware' threat category..... | 29 |
| 4.2.6 | Research findings on the assessment of the 'Theft of credential' threat category | 30 |
| 4.2.7 | Research findings on the assessment of the 'DDoS' threat category..... | 32 |
| 4.2.8 | Research findings on the assessment of the 'Human error' threat category..... | 32 |
| 4.2.9 | Research findings on the assessment of the 'Using outdated IT' threat category..... | 35 |
| 4.2.10 | Summary of the risk values of maritime cyber threat categories and threats..... | 37 |
| 4.3 | Research findings on 3D risk matrix | 38 |
| 5. | Discussion and conclusions..... | 40 |
| | References..... | 42 |
| | Appendix A : Example of vessel functions and related OT systems | 49 |
| | Appendix B : Example of different consequences in maritime cybersecurity | 51 |
| | Appendix C : First-run questionnaire | 53 |
| | Appendix D : Second-run questionnaire..... | 57 |
| | Appendix E : Deliverable 3 (Conference paper)..... | 61 |
| | Appendix F : Deliverable 4 (Presentation in AGA20)..... | 69 |

List of figures

| | | |
|---------|---|----|
| Fig. 1 | Cybersecurity process components | 11 |
| Fig. 2 | Flowchart of Cybersecurity barrier management | 13 |
| Fig. 3 | Example visualisation of cybersecurity Bow-Tie components | 13 |
| Fig. 4 | Barriers against malware | 13 |
| Fig. 5 | Barriers against DoS attack | 13 |
| Fig. 6 | The phishing Bayesian Network | 18 |
| Fig. 7 | Example of 3D risk matrix | 21 |
| Fig. 8 | Flowchart of the methodology | 22 |
| Fig. 9 | Result of the assessment of the 'Phishing' threat category | 25 |
| Fig. 10 | Result of the assessment of the 'Malware' threat category | 27 |
| Fig. 11 | Result of the assessment of the 'Man-in-the-middle' threat category | 28 |
| Fig. 12 | Result of the assessment of the 'Ransomware' threat category | 29 |
| Fig. 13 | Result of the assessment of the 'Theft of credential' threat category | 31 |
| Fig. 14 | Result of the assessment of the 'DDoS' threat category | 32 |
| Fig. 15 | Result of the assessment of the 'Human error' threat category | 34 |
| Fig. 16 | Result of the assessment of the 'Using outdated IT' threat category | 36 |
| Fig. 17 | Three-Dimensional scatterplot of maritime cyber threats | 39 |

List of tables

| | | |
|----------|--|----|
| Table 1 | Maritime cyberattack incidents | 6 |
| Table 2 | Cybersecurity Bow-Tie element descriptions | 14 |
| Table 3 | Linguistic scale for each parameter | 16 |
| Table 4 | Indices of Likelihood, Severity and Probability of Unpredictability | 16 |
| Table 5 | The established FRB with a belief structure | 19 |
| Table 6 | The conditional probability table (CPT) for the risk in the sub-FMEA based BN | 20 |
| Table 7 | Results of expert judgement | 23 |
| Table 8 | Respondents' background | 24 |
| Table 9 | Risk values of threat categories and threats | 37 |
| Table 10 | Threats' likelihood, consequence, and probability of the failure being undetected | 38 |

Evaluating cybersecurity in the maritime industry

Theme:

Maritime Cybersecurity

Liverpool John Moores University (Contractor)

And

Australian Maritime College, University of Tasmania

Chia-Hsun Chang

Senior Lecturer, Liverpool John Moores University, c.chang@ljmu.ac.uk

Wei Zhang

Lecturer, Australian Maritime College, University of Tasmania, vera.zhang@utas.edu.au

Wenming Shi

Lecturer, Australian Maritime College, University of Tasmania, Wenming.Shi@utas.edu.au

Changki Park

PhD student, Liverpool John Moores University, c.park@ljmu.ac.uk

Abstract Cybersecurity has become an important issue in the maritime industry due to many reported cyberattack incidents that caused a lot of economic loss, personal or company information breach, and so on. However, there is limited research for maritime cybersecurity in the existing literature. This research aims to conduct a risk assessment for cybersecurity in the maritime sector. In order to achieve that research aim, the definition of cybersecurity and current maritime cybersecurity issues are firstly reviewed. Following that, 34 cyber threats under eight cyber threat categories in the maritime industry are identified through systematic literature review. To deal with the identified threats, seven risk control options are also identified. A questionnaire is designed based on the literature review and distributed to validate the identified cybersecurity threats and explore more that are not identified during the literature review. Based on the results of the questionnaire, several top threats under each threat category are selected to conduct another questionnaire to collect the likelihood, consequence, and probability of failure detection with degree-of-belief-based five-point Likert scale. Through a rule-based Bayesian Network analysis, we found that the category of “Phishing” and the threat of “Connecting your infected USB or removable media to connect computers/navigation systems” contribute the most to the maritime cybersecurity risk.

Keyword: *Cybersecurity; maritime industry; risk management; Ruled-based Bayesian Network.*

Executive summary

Cybersecurity has recently received considerable attention in the maritime industry due to many reported cyberattack incidents that caused a lot of economic loss, personal or company information breach. In order to mitigate the effects of maritime cyber-attacks, this research aims to conduct a comprehensive risk assessment for cybersecurity in the maritime sector and proposes the following three research objectives: 1) To identify threats related to maritime cybersecurity; 2) To evaluate cybersecurity risk; 3) Provide some risk control options for maritime cyber threats.

To achieve the above three objectives, we conduct a systematic literature review and a first-run questionnaire with 31 experts in the maritime industry and academia, followed by a detailed investigation of the causes and consequences of the threats and a comprehensive discussion of potential solutions. Based on the results of the first-run questionnaire, eight maritime cyber threat categories are identified, including Phishing, Malware, Men-in-the-middle, Ransomware, Theft of credential, DDoS, Human error, and Using outdated IT. Each category includes several threats in detail. After that, a second-run questionnaire is further designed and conducted in this research to identify the cyber threats in the maritime industry and to collect their likelihood, consequence, and probability of failure detection with degree-of-belief-based five-point Likert scale. In addition, a variety of data analytical techniques, including Failure Modes and Effects Analysis (FMEA) with Rule-based Bayesian Network (RBN), and a three-dimensional (3D) risk matrix are used to quantify the cybersecurity risk in the maritime sector.

The main findings of this research are as follows. On one hand, a list of cyber threats and cyber threat categories are identified through a systematic literature review and validated by experts. As indicated, the category of “Phishing” contributes the most to the maritime cybersecurity risk, with the category’s value more than 40. By checking the aggregated raw data, the consequence of the three parameters (i.e. likelihood, consequence, and probability of the threat been undetected) have the highest values. This indicates that the maritime industry should try to find some methods either to mitigate the impacts of the consequences once phishing happens or to prevent them happen from reducing the likelihood or probability of the threat been undetected. However, the top values are just in the middle between UR₃ (27) and UR₄ (64), which indicates that most of the respondents feel that cyber threats do not significantly impact on the maritime industry. On the other side, the lowest cyber threat category is “Using outdated IT” with a value lower than UR₃ (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, we found that the likelihood of the three cyber threats are the lowest among the three parameters, which imply that most of the respondents believe that their companies have updated the IT to the latest version to protect the damage from the cyber-attacks.

On the other hand, from the cyber threat aspect, the most crucial one is ‘Accessing links from impersonation emails (e.g. bank, credit card company, insurance company, etc.)’, following by ‘Downloading attached files from impersonation emails (e.g. bank, credit card company, insurance company, etc.)’, and ‘Lacking knowledge of cybersecurity (i.e. facing a new situation and do not know how to deal with it) with threat values more than 40. Sea crews and company staffs 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 three cyber threats can all be avoided through high cybersecurity awareness, which is established by regular training and education.

Despite these significant findings, several limitations still exist in this research. First, we have limited replies from the target sample for both the first-run and second-run questionnaires. This might be due to the complicated questionnaires that are not easy to answer. We will collect more replies (e.g. expand the regions to other continents such as Asia and America) in the future to achieve acceptable replies numbers for further statistics analysis. Secondly, the respondents' background may be another factor that impacts on the reliability of the result. However, all respondents have some experience related to cybersecurity issues, although maritime cybersecurity is an emerging issue and everyone has different experience with such issue. Yet, the future research can conduct analysis with different weighting for people with different levels of familiarity to the maritime cybersecurity. Thirdly, although there were some operation technology (OT) items listed in the first-run questionnaire, their mean values are not higher than the threshold and thus are not listed in the second-run questionnaire. The second-run questionnaire is used to evaluate the cyber threats with three parameters (likelihood, consequence and probability of failure undetected), it will be more appropriate to list relative important threats based on the results of the first-run questionnaire to increase respondents' willingness answering the questionnaire. Apart from that, most of OT systems will transfer the signal to IT systems and thus the results can be deemed as a further risk assessment. However, the significant impact of OT system are also vulnerabilities to maritime cybersecurity and need to be considered as well. For the further research, it is suggested to address more on OT perspective to fill the gap. Fourthly, the consequence can be different types. In our research, the consequences are aggregated. For further research, there is a need to investigate the details of different consequence types to analyse the consequence from different aspects. All these point out the potential direction for the future research.

FY2019 IAMU Research Report

Evaluating cybersecurity in the maritime industry

1. Introduction

1.1 Background

According to [1], there are around 80% of international trade transported by ships. Meanwhile, the increasing relay on information communication technology in international trade has attracted more concerns on cybersecurity to the maritime industry. For example, Port of Antwerp suffered cyberattack by drug smugglers in 2011 and 2012, Maersk has lost \$200~300 million by cyberattack in 2017, and COSCO terminal at Port of Long Beach has also suffered a cyberattack in 2018. With such increasing concern on maritime cybersecurity, International Maritime Organization (IMO) and Baltic and International Maritime Council (BIMCO) have published several maritime cybersecurity guidelines recently. IMO proposed a cybersecurity guideline (MSC-FAL.1/Circ.3) in 2017; whereas BIMCO published a cybersecurity guideline for onboard ships in 2016. These guidelines referred to NIST and ISO/IEC 27001 as a source of additional guidance and standards [2]. Although there are increasing maritime cyber-attack incidents and several maritime cybersecurity guidelines provided by international organisations, studies that addressed on maritime cybersecurity risk assessment is still at a beginning stage and is ten to twenty years behind other computer-based industries [3], such as aviation ([4], [5], [6]), healthcare [7], etc.

1.2 Research aim and objectives

Based on the above statement, the author has found out a lack of research addressing cybersecurity in the maritime industry. Therefore, cybersecurity needs to be addressed with more attention and precautions for the maritime industry. In order to facilitate the research on maritime cybersecurity, this research aims to conduct a risk assessment for cybersecurity in the maritime sector. In order to achieve the research aim, three research objectives are proposed as follows: (1) To identify threats related to maritime cybersecurity. It will be identified through a systematic literature review, and interview with experts in the maritime industry and academia. (2) To evaluate cybersecurity risk. For this, a detailed investigation of the causes and consequences of the threats will be approached. A Bayesian Network model will be built up and can be updated and/or expanded for further research. This is the main contribution of this report. (3) Provide some solutions to controlling the identified risk factors. This will be identified through a systematic literature review.

1.3 Significance of this research

Research for cybersecurity in maritime is at the beginning stage Cybersecurity risk assessment research in the maritime industry is limited. [26] published a model-based framework for maritime cyber risk assessment, but their work does not involve risk control options. This study systematic reviews the cybersecurity in the maritime industry. A set of risk control options for the maritime cybersecurity will also be proposed and evaluated. Furthermore, this study will establish a framework for cybersecurity risk management in the maritime industry that can be used as a reference for further research related to maritime cybersecurity.

1.4 Report structure

The rest of this report is structured as follows: Section 2 presents a systematic literature review with the identification of cybersecurity threats and risk control options in the maritime industry, while section 3 describes the methodology. Section 4 presents the results of data analysis, and discussion and conclusion are drawn in section 5.

2. Literature review

2.1 Definition of Cybersecurity

Cybersecurity is defined as “the protection of cyberspace as well as individuals and organizations that function within cyberspace and their assets in that space” [8]. In the maritime area, ISPS code proposed by IMO defined that “cybersecurity is one of the tool, practice policy, safety concept, technologies, and process designing for protecting network system, computers, programs and its data from intended or unintended arrack, damage, contaminated program, or unauthorized use, access, or modulation”.

Cybersecurity threat is defined as the factors that cause cyber-risk [55]. Various cybersecurity threats are found along with the development of advanced information communication technology. In recent years, many cyberattack incidents are reported with some common cyber threats such as phishing, malware, ransomware, DDoS, man-in-the-middle attack, and so on ([9], [10], [11]).

2.2 Maritime cyberattack incidents

Many maritime cyberattacks have been reported from 2011 because the maritime industry is more and more rely on the advanced information and communication technology in navigation at sea and communication with supply chain partners. According to [58], maritime cyber threats have increased due to: i) increasing connectivity of ships, ii) ever-greater integration of ICS into on board networks, iii) pre-internet systems and protocols wrapped in IP, iv) widespread use of USB memory devices for data sharing, v) greater use of remote access capability, vi) attackers increasingly targeting non-conventional IT, vii) lack of leadership in the maritime cyber security space. For instance, Port of Antwerp suffered cyberattack from drug traffickers [12]; 280 South Korean vessels were cyberattacked to their navigational system and the GPS signal was jammed [13]. The most well-known case is Maersk was cyberattacked by a ransomware in 2017 and caused a \$200-300 million financial lose in three-weeks network system shutdown [14]. In 2018, there are more maritime cyberattack incidents, e.g. COSCO terminal at the Port of Long Beach was also cyberattacked with 5 days shutdown and less financial loss, as they took a lesson from Maersk incident in 2017 [15]. Other cases include Port of Barcelona’s security infrastructure [16], San Diego Port’s incident impacting on park permits, public records requests and general business services [17], Ukraine vessels cyberattacked by Russia [18], Australian shipbuilder’s ship designs were stolen [19], U.S Navy’s ship maintenance data and missile plans were repeatedly stolen by Chinese hackers [20]. In 2019, the U.S. Coast Guard issued a warning after it received a report that a merchant vessel had its networks disrupted by malware while travelling through international waters [21]. A list of detailed information about maritime cyberattacks can be found in Table 1.

Table 1 *Maritime cyberattack incidents*

| Year | Organization | Details |
|-----------|--------------------------------------|--|
| 2011 | IRISL | An Iranian shipping line, IRISL, was cyberattacked in 2011 and lost all data related to rates, loading, cargo number, date and place. |
| 2011-2012 | Port of Antwerp | Drug traffickers hired hackers to breach IT system of Port of Antwerp. Hackers accessed secure data giving them the location and security details of containers which contained heroin and cocaine. |
| 2012-2014 | Danish Maritime Authority | Danish Maritime Authority was subjected to a cyberattack from 2012 but been discovered until 2014. The attack was introduced by a PDF document infected with a virus, and the virus was propagated from the Danish Maritime Authority to other government institutions. |
| 2013 | Mobile Offshore Drilling Unit | A group of hackers remotely attacked a floating oil rig off the Gulf of Mexico and gained control of its stabilization systems and programmed the platform to tilt dangerously to one side. The platform had to be shut down for 19 days. |
| 2016 | Korean vessels | South Korea reported that 280 vessels suffered problems with their navigational systems. The GPS signal was jammed by hackers; consequently, some of the GPS signals died and others received false information. |
| 2017 | Maersk | Maersk, the largest container shipping company in the world, was cyberattacked by a ransomware (NotPetya) in 2017, which shut downed Maersk's network system. It took almost three weeks to recover and caused a \$200-300 million financial loss. |
| 2018 | COSCO terminal at Port of Long Beach | COSCO terminal at the port of Long Beach has been attacked by ransomware in July 2018 and took 5 days to recover. However, they did not suffer serious financial loss, as they took a lesson from Maersk incident in 2017 and separated their network in different servers. |
| 2018 | Port of Barcelona | Hackers attacked several servers in the port's security infrastructure, without interrupting the maritime and land operations. |
| 2018 | San Diego Port | The attack had not stopped vessels or boat using the port, or put members of the public in danger. The main impact would be on the issuing of park permits, public records requests and general business services. The Port said some of the disruption was because of staff shutting down computers that were in danger of being compromised as the ransomware started to spread. |
| 2018 | Ukraine vessel | Security researchers report that Russia launched coordinated cyberattacks against Ukrainian government and military targets before and during the attack on Ukrainian ships in late November. |
| 2018 | Australian shipbuilder | Australian defence shipbuilder Austal announced it had been the victim of a hack resulting in the theft of unclassified ship designs which were later sold online. |
| 2018 | U.S Navy | U.S. Navy officials report that Chinese hackers had repeatedly stolen information from Navy contractors including ship maintenance data and missile plans. |
| 2019 | U.S merchant ship | The U.S. Coast Guard issued a warning after it received a report that a merchant vessel had its networks disrupted by malware while traveling through international waters. |

2.3 Cybersecurity threats in the maritime industry

Based on the existing literatures related to maritime cybersecurity, the cyber threats are mainly from human elements and external systems attack. In this research, they are categorised into eight groups, including human error, using outdated IT system, malware, phishing, man in the middle attack, ransomware, theft of credential, and distribute denial of service (DDoS). The details are described as follows:

2.3.1 Human error

For shipping safety and security incidents, human error has been recognised as the most critical factor that causes around 80-90% of shipping accidents directly and indirectly ([22], [23]). In the maritime cybersecurity section, human error is also pointed out as a main threat to maritime cybersecurity [24].

2.3.2 Using outdated IT system

[25] and [26] analysed vulnerability of maritime cybersecurity and found that shipping companies were over reliance on outdated technology and security practices, which might cause a major problem. For instance, maritime employees still believe that firewalls and antivirus software are sufficient to deal with cyberattacks. Without up-to-date IT systems, hackers can attack vessels or companies through viruses or other assorted malware, which are difficult to be detected and defended by traditional antivirus software [25]. On the other hand, as large ships are expensive and take a long time to build, many ships were built before cybersecurity as a major concern. Thus, some vessels are still operating through outdated software systems that might cause cyberattack [26].

2.3.3 Malware

Malware is a malicious software that assesses or damages devices without the knowledge of the device's owners, and further spread virus by opening infected email attached files or accessing a fake website with malicious malware such as Trojan horses, worms, exploits and backdoors [27]. In the maritime sector, [28] and [29] have also listed malware as a severe threat to maritime cybersecurity as malware could access and damage vessel's operation system or steal sensitive data from the shipping companies. Malware threats can attack navigation system even with non-data USB (e.g. an e-cigarette) via any port capable of reading data [56]. This is a very likely scenario as most people do not aware that the malware attacks can be conducted in such way and take it lightly.

2.3.4 Phishing

Phishing refers to sending a seemingly legit email with links to fake websites or to download malicious files. The email may show that it is from a bank or other various legitimate business. 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 private devices (e.g. smart phone, tablet, personnel USB device, etc.) could cause cybersecurity issues through phishing emails or accessing fake websites, and thus installing malicious virus into vessel operational system ([30], [31], [32], [28]).

2.3.5 Man in the middle attack

Through man in the middle attacks, hackers can obtain all the communication between different parties and pretend to be the parties. Hackers hide their presence and stop the users from sending and receiving data, or might even divert and redirect the messages to another user [33]. In the maritime industry, such

cyber threat commonly attacks remote desktop protocol (RDP) service running on the Electronic Chart Display and Information System (ECDIS) [34].

2.3.6 Ransomware

Ransomware attacks refer to encrypt and lock the files on a computer until the ransom is paid [35]. Ransomware attacks may result in economic loss or costs of rebuilding lost data [66]. Ransomware used to attack traditional computing systems as well as mobile devices, and could be adapted to the maritime domain. Recently, the incidents of ransomware are increasing again, with a 165% increase of new Ransomware in the first quarter of 2015 [36] showing that it is a highly profitable and growing sphere of criminal activity [26].

2.3.7 Theft of credentials

Theft of credential is a type of cyber threat that stealing the proof of identity from users or customers [37]. [38] proposed that some threat actor groups may break into server or website to steal user's credentials.

2.3.8 Distribute Denial of Service (DDoS)

In the maritime sector, targeted attacks usually use tools and techniques specifically created for a company or ship, which include brute force, Denial of Service (DoS), or Distribute Denial of Service (DDoS) [28]. A DoS attack makes a system or network resource unavailable to its intended users (deny the service). A coordinated DoS attack from multiple sources is called a distributed denial of service attack (DDoS). Either of these may also be executed to camouflage other attacks, such as espionage or hacking [59]. DoS and DDoS attack refer to a serious attack that will disrupt a ship's operation and network system, such as global positioning system (GPS), radio detection and ranging (RADAR), and autonomic identification system (AIS) [39]. Craiger and Haass [61] organised several studies (i.e. Parker, [62], Gauthier and Seker [63], Strohmeier et al. [64]) and summarised 16 cyber threats related to AIS, including GPS jamming, GPS failure/poor transmission, AIS device off, AIS malfunction, AIS bad data, AIS jamming, AIS bit errors, Vessel spoofing, Eavesdropping, Flooding, Ghost vessel, CPA/AIS-SART spoofing, Disappearance, AtoN spoofing, Data diddling, and Weather spoofing.

2.4 Risk control options for maritime cybersecurity

There is no one regulation or standard for maritime systems and cyber security [65]. Maritime cybersecurity poses a unique set challenges for regulators to consider. The establishment of a cyber code for global maritime industry is needed to speed up the development of cyber security standards and support effective and holistic maritime cyber risk management. However, IMO- Maritime Safety Committee (MSC), Sub-Committee on Navigation, Communication and Search and Rescue (NCSR) and Facilitation Committee (FAL) have provided many guidelines for it. For example,

- MSC95/4/1: Industry guidelines on cyber security on board ships, submitted by ICS, BIMCO, INTERTANKO and INTERCARGO, 5 March 2015.
- MSC95/4/2: International Ship and Port Facility Security (ISPS) Code cyber security provisions, submitted by Canada, 18 March 2015.
- NCSR1/INF.5: Background information related to the development of e-navigation, submitted by Norway, 28 March 2015.
- NCSR1/9: Report of the correspondence Group on e-navigation, submitted by Norway, 28 March 2015.

- MSC95/INF.19: Cyberphysical relationship in port security – CYSM project, submitted by the European Commission, 14 April 2015.
- E-Navigation Strategy Implementation Plan, approved by MSC 94, November 2014.
- FAL40/INF.4: The Guidelines on Cybersecurity on board Ships, submitted by ICS, BIMCO, INTERTANKO, CLIA and INTERCARGO, 30 December 2015.
- MSC96/4/1: The guidelines on cyber security onboard ships, submitted by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO and IUMI, 4 February 2016.
- MSC.1/Circ.1526: Interim Guidelines on Maritime Cyber Risk Management, 1 June 2016.
- MSC98/WP.9: Measures to enhance maritime security, Report of the Working Group, 15 June 2017.
- Resolution MSC.428(98): Maritime cyber risk management in safety management systems, adopted 16 June 2017.
- MSC-FAL.1/Circ.3: Guidelines on maritime cyber risk management, 5 July 2017.
- NCSR5/22/4: Industry standard on software maintenance of shipboard equipment, submitted by BIMCO and CIRM, 14 December 2017.
- MSC101/4/1: The industry guidelines on cyber security on board ships, version 3, submitted by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, CLIA, INTERCARGO, InterManager and WSC, 11 March 2019.

Many other organisations are also addressing maritime cybersecurity and provided some documents for improving it, such as BIMCO, DNV GL [59], Danish Maritime Authority (Cyber and information security strategy for the maritime sector 2019-2022, January 2019), Marsh (The risk of cyber-attack to the maritime sector, July 2014.), US Coast Guard (Navigation and Vessel Inspection Circular (NVIC) 05-17: Guidelines for addressing cyber risks at MTSA regulated facilities, 12 July 2017; Safety Alert 06-19: Cyber incident exposes potential vulnerabilities onboard commercial vessels, 8 July 2019.), EU (EU Directive 2016/1148; European Insurance and Occupational Pensions Authority (EIOPA): Cyber risk for insurers – challenges and opportunities, 2019.), Digital Container Shipping Association (Cyber security guide, March 2020), UK Department for Transport & Maritime and Coastguard Agency (Port cyber security code for operations and staff members, 16 August 2016), and so on.

Apart from the above guidelines and documents for maritime cybersecurity, there are a number of studies addressing maritime cybersecurity treatments and can be roughly categorised as follows:

2.4.1. Cybersecurity education and training

Cybersecurity education and training to employees is an important risk control option (RCO) and has been emphasized in many industries, such as health care [54], bank [40], etc. For example, [54] proposed that well trained employees can have effective role as a “human firewall” to protect asset. [40] insisted that since finance staffs overlook sensitive and confidential finance data, through cyber security education, bank employees need to recognize cybercrimes and respond appropriately.

In the maritime sector, in order to deal with the threats from human error, training and educating sea crews and staffs may be an effective method to enhance maritime cybersecurity. [26] suggested that sea crews should be educated to deal with of cyberattack by password protection and access keys. Companies need to train their staffs and sea crews how to use digital equipment in a correct way, which can not only reduce the damage to the equipment, but also protect from cyberattacks. An event tree or standard operation process should be established to guild the staffs and sea crews to avoid or deal with cyberattacks. Shipping companies should also follow the suggestion from IMO STCW (International Maritime Organization Standards of Training, Certification, and Watchkeeping) code and ISM

(International Safety Management) code to enhance maritime cybersecurity. Those codes require shipping companies to take cyber risk management system in the approved safety system. DNV GL [59] also provided several treatments related to cybersecurity training, such as Training staff before actual use of a program, Training on security safeguards and maintenance and administration staff, etc. For more information about maritime cybersecurity education and training can be found in [67].

2.4.2 Malware protection software installation

Installing anti-virus programme is an important process to protect system and data from cyberattack. For example, in the banking industry, antivirus tools are used to protect the bank's system and network from malicious attacks [40]. [41] stated that it is necessary to apply antivirus software for protecting data in the healthcare industry, especially for the regulation of the General Data Protection Regulation (GDPR) for personal data protection. In the maritime area, [28] found that because of failure software maintenance and patching, the number of maritime cyber incidents increase to a notable situation. They insisted that malware software and anti-virus should be installed and updated on all work-related computers on board to reduce the possibility of being cyberattacked.

2.4.3 Software update

In order to deal with the threat of the use of outdated IT system, it is necessary to keep updated vaccine software and use updated programmes to mitigate cyber risk [42]. This is because through the development of advanced technology, many virus and malicious program are also created simultaneously. The maritime industry needs to update or even upgrade IT system for not only keep their competitiveness, but also deal with the threat from cyberattacks. [43] stated that highest degree monitoring and the capabilities of defensive to various cyberattacks are important when upgrading the network and software systems.

2.4.4 Password policy

Password policy is a low-cost and easily implemented measure against cyber threats by avoiding using the same or simple password, yet it needs to get the awareness from governments and individual [44] [59]. In the finance sector, this policy is applied to both employees and customers. [40] stated that a secure password can protect personal data against cyberattacks from phishing and identity theft. [30] stated that a secure password practice onboard cybersecurity access control should be strong, reset periodically, and disable automatic saving. [29] warned that a weak password might cause unauthorized access and cause a data breach. Therefore, to mitigate the risk, a password policy should be created and employees should be trained to comply with that policy [45].

2.4.5 Developing cybersecurity process

[29] recommended five functional elements that support effective cybersecurity process as follows:

- Identifying - define personnel roles and responsibilities for cyber risk management,
- Protecting - implement risk control processes and planning to protect against cyberattack
- Detecting - develop activities necessary to detect cyberattack in a timely,
- Responding - develop activities and plans to provide resilience and restore systems
- Recovering – identify measure to back up and restore cyber systems for operation impacted by cyberattack

[28] also proposed a six-step cyber risk management approach shown as Fig. 1.

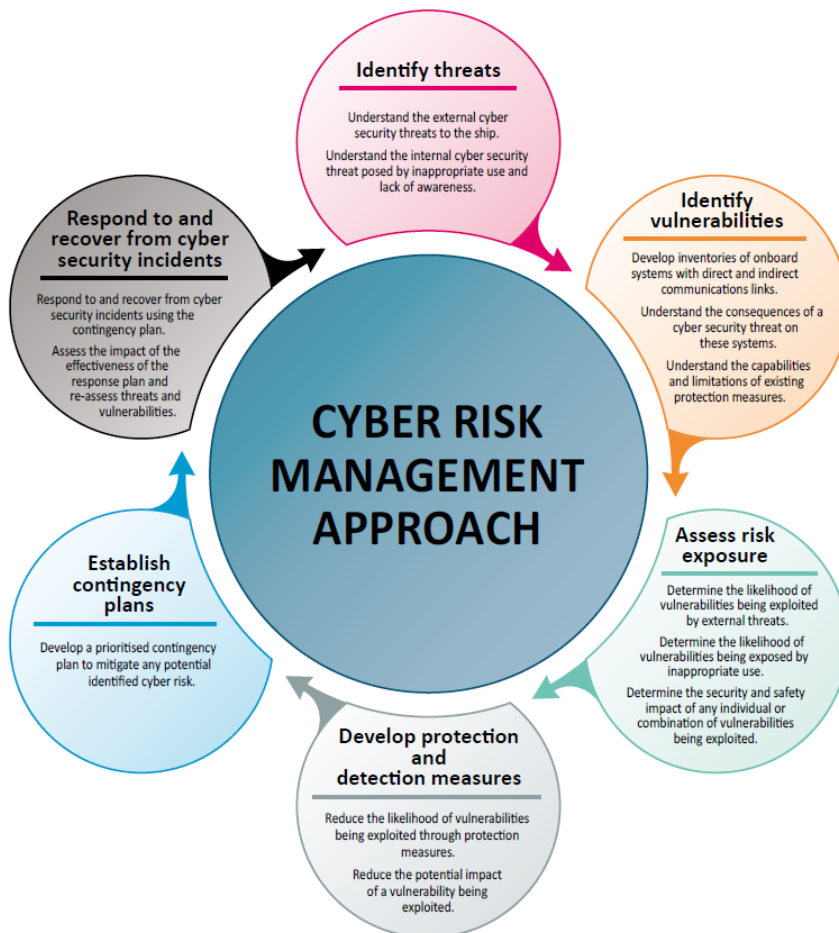


Fig. 1 Cybersecurity process components

Source: [28]

In fact, there were some changes in cybersecurity process after a huge cyber incident such as Maersk in 2017. For example, COSCO divided data in several servers and thus cut down the connection of the infected server and operated through other non-infected servers when they faced the cyberattack in 2018. In addition, because of their quick response and notification to customers, they suffered a relatively lower impact from this cyberattack [15]. In fact, cybersecurity responsibility should be shared by different participants of the value chain, including owners of the vessel or offshore assets, users of the different systems, respective suppliers as well as ship managers and the operators themselves [59]. DVN GL [59] also suggested that senior management should carry the overall responsibility and establishes the risk management policies.

2.4.6 Enhancing cybersecurity awareness

In the past time, cyber threats were not recognised as a high-risk. This can be found in a survey conducted by a shipping company (Sea Asia Company) in 2017, and the result showed that only 43.75% of shipping companies set up some prevention activities or programmes to protect against cyber threats and thus minimising losses. BIMCO (2018) stated that the shipping line, which lacks cyber awareness

training and governance in their own system, may represent more source of vulnerabilities, and could result in cyber incidents. Therefore, IMO decided in MSC. 428 (98) which is to enhance cybersecurity awareness, shipping company requires a cyber management system to be included in the approved safety management system, from 1st of January, 2020. Therefore, seafarers should be sufficiently qualified in their capacity on board for cyber security awareness before assigning the duties. [57] also provided several examples of how to recognise fake emails, such as unknown sender (even if the sender is someone we might know, but the content seems to be out of place), Greeting (the greeting only uses something general such as “Dear member” rather than directly mention our name), Phone number (should check the phone number before calling it), Spelling and grammar mistakes, and Hyperlinks in the email. DNV GL [59] also proposed a list of cybersecurity treatments for enhancing cybersecurity awareness, such as Staff awareness on information security concerning, Making staff aware of information security issues, etc. IMO [60] stated that effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organisation and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

2.4.7 Firewall, web and mail content filtering and proxy server

Using firewall, content filtering and proxy server can bring several benefits to enhance cybersecurity. For example, it prevents malicious web sites from any access through the proxy server [46]. Moreover, content filtering application scan e-mail, corporations are wide open to productivity-robbing attacks from advertisers, malicious virus programmers, and pornography promoters [47]. DNV GL [59] also proposed a list of cybersecurity treatments related to firewall and security gateway, such as Integration of proxy servers into the security gateway, Use of a logging server on a security gateway, Integration of virus scanners into a security gateway, Secure use of protocols and services, and so on.

2.5 Cybersecurity barrier management

The Bow-Tie analysis is proposed by DNV GL [59] and applied in the cybersecurity barrier management. The method incorporates both the event tree and fault tree analysis. The four steps in this process includes: 1) identifying the threats to system which supports specific vessel functions and business processes; 2) identifying incident prevention barriers; 3) identifying consequence reduction barriers; and 4) assessing the robustness and effectiveness of these barriers mentioned in 2) and 3) above. The detailed illustration shows in Figure 2.:

Detailed illustrations of this approach are presented in Figure 3. Figure 3 shows the barriers (grey boxes in the left of the figure) to prevent the threats (blue boxes) and the mitigation barriers (grey boxes in the right of the figure) to prevent the consequences (red boxes). It can be observed that the Bow-Tie approach focuses on the communication and building the awareness on cybersecurity efforts, without emphasising on the probability or frequency. It aims to assess risks and address controls and barriers against the cyber-attacks. It also includes the general concepts of the NIST five framework core functions (ref. /34/) also referenced in the BIMCO guideline on cybersecurity.

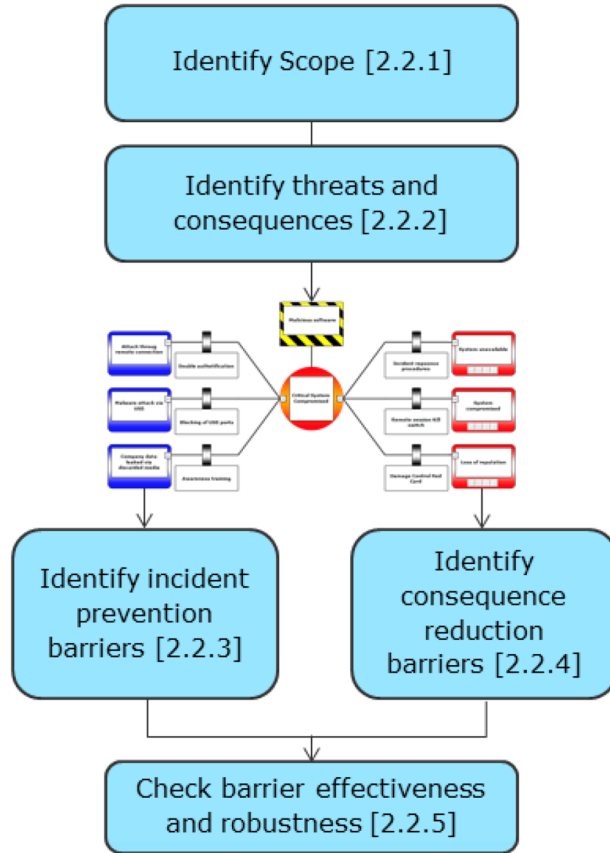


Fig. 2 Flowchart of Cybersecurity barrier management

Source: DNV GL [59]

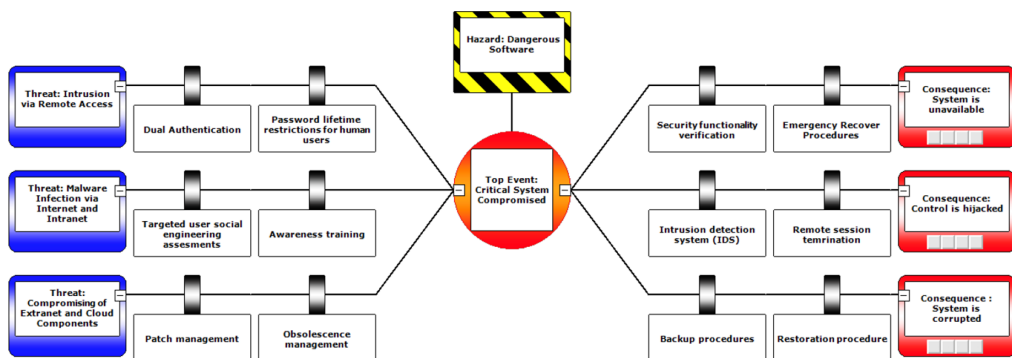


Fig. 3 Example visualisation of cybersecurity Bow-Tie components

Source: DNV GL [59]

There are five main elements/components of cybersecurity risks in the Bow-Tie method, i.e. hazards, top events, threats, consequences and barriers. Table 2 describes the main elements of the cybersecurity Bow-Tie method and their description and examples.

Table 2 Cybersecurity Bow-Tie element descriptions

| CS Bow-Tie element | Description and examples |
|-----------------------|--|
| Hazard | An entity with the potential to cause harm, but also being necessary for performing the business. Samples used in this RP refer to software which is business critical, but notorious for being infected with viruses, malware and Trojan traps. |
| Top event | As long as a hazard is controlled, the top event does not occur. It is the event that shall be avoided, for example: The event when the critical system is compromised. Ex. infections, intrusions, successful password hacking, security breach. |
| Threats | Threats are categorised as unintentional and intentional attacks from internal or external attackers exploiting vulnerabilities such as the top 10 threats listed by the BSI ref. /29/: <ul style="list-style-type: none"> – malware infection via internet and intranet – introduction of malware on removable media and external hardware – social engineering – human error and sabotage – intrusion via remote access – control components connected to the internet – technical malfunctions and force majeure – compromising of smartphones in the production environment – compromising of extranet and cloud components – (D)DoS attacks. |
| Consequences | The outcome of an unwanted event (occurrence of the top event). Examples: system is down, control is hijacked, damage to infrastructure due to resulting malfunctions. |
| Barrier | Any measure taken that acts against some undesirable force or intention, in order to maintain a desired state. There are two types of barriers: <ul style="list-style-type: none"> – Proactive or preventive barriers (left side of the top event) that prevent the top event from happening. For example: PSWD lifetime restrictions for human users, dual authentication, targeted user social engineering assessments, awareness training, patch management, obsolescence management, USB management policies. – Reactive or mitigating barriers (right side of the top event) that prevent the top event resulting into unwanted consequences. For example: security functionality verification, remote session termination, intrusion detection systems (IDS), emergency recovery procedures, backups, restoration procedures, spare parts. |

Source: DNV GL [59]

Several examples are also provided in the report of DNV GL [59]. Figure 4 demonstrates the example of malware. It illustrates three ways of showing how the malware gets into the system, including spread through network, spread through removable storage, and spread through user behaviour. In particular, social engineering plays an ever-increasing role in exploiting the weaknesses of user behaviour. From Figure 4, it can be clearly seen that network segregation and traffic limit between network segments are barriers to prevent a worm. In this sense, only defined traffic (protocols) and nodes (addresses) are allowed. It should be mentioned that, for larger information systems, special intrusion prevention systems (IPS) are available, which recognise and block known malicious patterns but IPS may not be suitable for industrial control systems. On the other hand, to efficiently avoid threats from malware, it is commonly believed that the installation of anti-virus and anti-spyware software is mandatory for all malware threats. For example, it is applicable and efficient to update the signatures continuously. This may raise a further issue with respect to manual procedures for updating anti-virus and spyware software for ships. The primary reason is limited data traffic to ships due to segmentation and limited bandwidth. After testing those changes, system hardening and patch management are further identified as needed barriers for malware, particularly for critical systems. Lastly, to get a better understanding of the installed patches in all components, a software patch inventory system is essential.

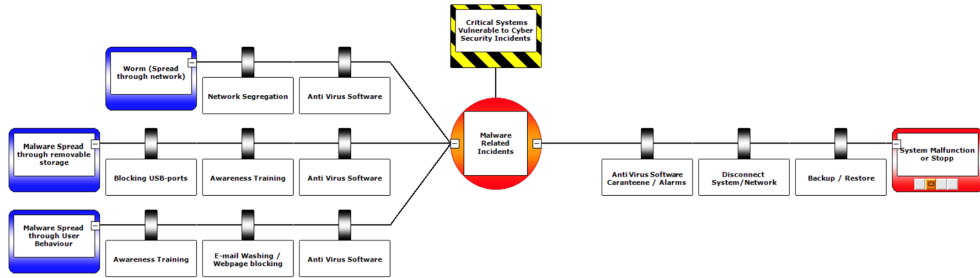


Fig. 4 Barriers against malware

Source: DNV GL [59]

Taking DoS attack an example, DNV GL [59] illustrated demonstrated another scenario and demonstrated it in Figure 5. As seen, three ways are usually used by the attacker, such as flooding the network, flooding buffers in devices by stating buffers in the firewall, and flooding the application by doing frequent resource intensive operations. First, network segregation and traffic limit are commonly believed to be efficient barriers to prevent a network flooding threat. In this sense, it is required to allow only a minimum of defined traffic (protocols) and nodes (addresses). Second, to avoid the occurrence of buffer flooding, special devices can be applied, which is believed to be efficient to block DoS attacks (cleaning centres or scrubbing centres). Regrettably, these special devices are mainly targeted at larger information systems, making them less attractive for control systems onboard a ship, offshore rig or terminal. Regarding malware barriers, it has been widely recognized that software updates and patch management are particularly important. Also, hardening of systems plays a significant role in reducing all types of attacks. It is worth mentioning that the use of security certified devices is believed to be typical barriers to prevent buffer flooding, which can configure the devices according to certificate requirements. Third, to prevent application flooding efficiently, a fundamental action is to build resistance into the application design. A further action is to implement strong user authentication and authorisation. These actions can help to develop an effective barrier to application flooding. On the other hand, the consequences of a DoS attack are always a considerable concern for stakeholders in the maritime industry. To reduce the consequences, a necessary step is to identify the unwanted traffic, which can be achieved by using special intrusion detection systems (IDS) or DoS detection systems. However, these systems may not be suitable for the smaller shipboard and offshore industrial control systems, which requires other alternative approaches. A typical approach is to use simpler devices. In so doing, it not only monitors the network traffic efficiently but also establishes procedures for monitoring these logs. When detecting abnormalities, further actions will be taken to block the source network and restore systems.

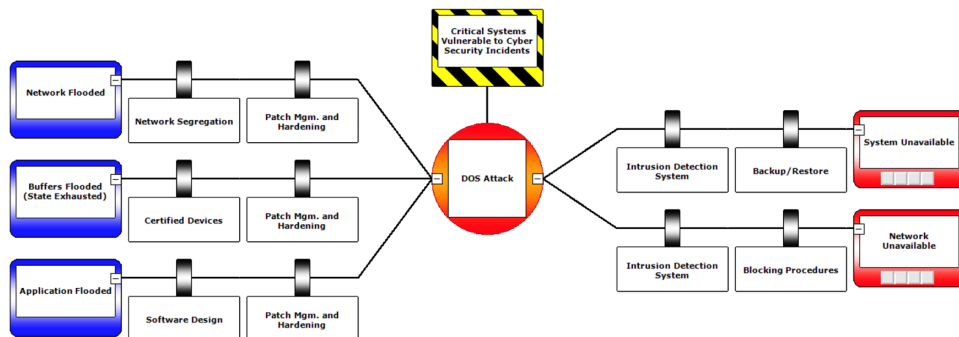


Fig. 5 Barriers against DoS attack

Source: DNV GL [59]

3. Methodology

From the above section, a thorough literature review has been performed. Cyber security related threats have been identified based on the literature review and a questionnaire (see Appendix A). Another questionnaire has been designed to collect information for the assessment of risks based on Rule-based Bayesian Networks (see Appendix B).

3.1 Data collection

In order to validate the identified threats and explore more if they are not identified from the literature review, a semi-structure questionnaire (named: validation threat questionnaire) has been designed on Bristol online survey (<https://ljmu.onlinesurveys.ac.uk/cybersecurity-in-the-maritime-industry>) and distributed to experts work in port authorities, liner shipping companies, and academia.

A questionnaire is designed and distributed to collect the degree of belief (DoB) of the L, C and P for each threat. Compared with normal Likert scale questionnaire, DoB involves respondents' uncertainty when answering questions and thus provides more insights to the research. Respondents indicate the DoB with a percentage to which they endorse each statement using a five-point Likert scale; see Table 3 for the linguistic terms used for each parameter and Table 4 for their definitions. It is obvious that for any of the three parameters (L, C and P) the sum of the DoB of the five-level Likert item should be equal to 100%. For example, an expert might assess the likelihood of 'Accessing links from impersonation emails (e.g. bank, credit card company, insurance company, etc.)' to be 5% Medium, 10% Low, and 85% Very Low, and the consequences are 10% High, 40% Medium, 30% Low, and 20% Very Low.

Table 3 Linguistic scale for each parameter

| Parameter/Items | 1 | 2 | 3 | 4 | 5 |
|---|-----------------|----------|----------|----------|-----------------|
| L: likelihood | Very low | low | average | frequent | Highly frequent |
| C: severity | negligible | marginal | moderate | critical | catastrophic |
| P: probability of failure being undetected | highly unlikely | unlikely | average | likely | highly likely |

Table 4 Indices of Likelihood, Severity and Probability of Unpredictability

| Likelihood of failure | Definition |
|-----------------------|---|
| 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 | Definition |
|----------------------|--|
| 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 (e.g. less than 6 hours) |
| Moderate (MO) | Moderate system damage. Operations and production interrupted marginally, and resumed to its usual operational mode within more than 12 hours |
| Critical (CR) | Major system damage. Operations stopped. High degree of operational interruption |

| Consequence severity | Definition |
|----------------------|---|
| 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 | Definition |
|---|--|
| 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 |

Source: adapted from [48]

3.2 Data analysis method

Failure Modes and Effects Analysis (FMEA) with Rule-based Bayesian Network (RBN) to evaluate the importance of the maritime cybersecurity. They are used together because RBN is widely used to overcome the shortages of FMEA, which is discussed in Section 3.2.1.

3.2.1 Failure Modes and Effects Analysis (FMEA)

FMEA is widely used for the systematic evaluation of the severity of potential failure modes and is one of the most popular safety and reliability analysis tools for products and processes [48]. Risk Priority Number (RPN), the main component of FMEA, is multiplied by three factors, i.e. the likelihood of failure (L), its consequence severity (C), and the probability of the failure being undetected (P). The three factors are measured by five linguistic terms: very high ($i = 5$), high ($i = 4$), medium ($i = 3$), low ($i = 2$), and very low ($i = 1$). L is estimated by five linguistic terms ($Li, i = 1, 2, \dots, 5$): very low, low, average, frequent, and highly frequent. C is estimated by five terms ($Ci, i = 1, 2, \dots, 5$): negligible, marginal, moderate, critical, and catastrophic. P is estimated by five terms ($Pi, i = 1, 2, \dots, 5$): highly unlikely, unlikely, average, likely, and highly likely. The RPN is formulated as below:

$$RPN = Li \times Ci \times Pi$$

Although FMEA has been widely used in risk and safety assessments, the uses of RPN in risk assessments are criticised by several reasons ([48], [49]):

1. The results of RPN are produced with liner calculations, no weights of the provided evidence are used, and the relationships among variables are not considered.
2. It is difficult to give precise value for intangible quantities associated with L, C, and P.
3. The same value of risk priority number many indicate totally different risk implications (unable to provide a backward diagnose/inference).
4. The RPNs that are used for identifying the criticality factors strongly influence the result.
5. It cannot measure the effectiveness of corrective actions.

3.2.2 Rule-based Bayesian networks (RBN)

In order to overcome the shortcomings of FMEA listed in Section 3.2.1, [48] proposed a fuzzy-rule Bayesian reasoning mechanism, which involves five main steps as follows:

- (1) Establishment of FRB with belief structures in FMEA
- (2) Failure estimation and transformation
- (3) Rule aggregation using a Bayesian reasoning mechanism
- (4) Development of utility functions for failure ranking, and
- (5) Validation using benchmarking and sensitivity analysis

In our research, we introduce a five-step approach as follows:

- (1) Identify threats in maritime cybersecurity
- (2) Build up a Bayesian network
- (3) Establish rule-based systems with belief structure in FMEA-based BN
- (4) Rule aggregation using a Bayesian Reasoning mechanism
- (5) Convert the obtained results into crisp values by using utility functions

Step 1: Identify threats in maritime cybersecurity

Based on the results of literature review and the first run questionnaire, eight maritime cyber threat categories are identified, including phishing, malware, Men-in-the-middle attack, Ransomware, Theft of credential, DDoS, human error, and Using outdated IT system. Each threat category has several threats (see Table 6).

Step 2: Build up a Bayesian network

After identifying the threat categories and threats, they are further converted to build up a Bayesian network (BN). Figure 6 illustrates a developed BN by using the category of phishing as an example, threats are the root nodes (yellow nodes) and threat categories are the leaf nodes (orange nodes).

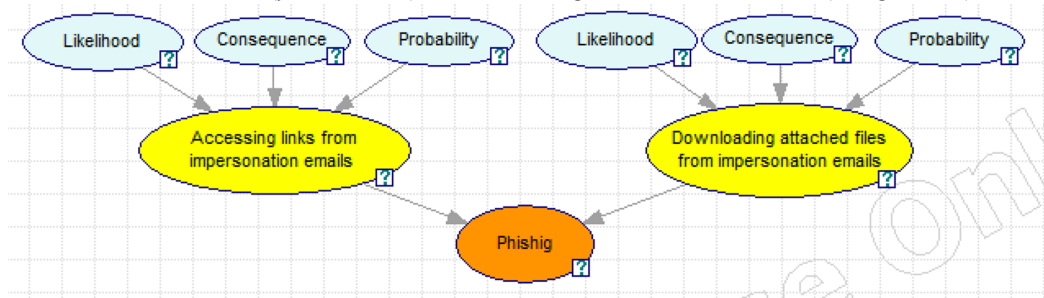


Fig. 6 The phishing Bayesian Network

Step 3: Establish rule-based systems with belief structure in FMEA-based BN

To describe the influential magnitudes of threats to the threat category, the risk model assigns a set of five linguistic states ($R_i, i = 1, \dots, 5$) as “very low”, “low”, “average”, “high”, and “very high” for the root nodes (threats) and the leaf node (threat categories). Meanwhile, the linguistic states for L, C, P that in the FMEA-based BN are also assigned, in which five grade linguistic variables for L are ‘very low’, ‘low’, ‘average’, ‘high’ and ‘very high’; for the consequence are ‘negligible’, ‘marginal’, ‘moderate’, ‘critical’ and ‘catastrophic’; and to estimate C, one may use such variables as ‘highly unlikely’, ‘unlikely’, ‘average’, ‘likely’, ‘highly likely’ (see Table 4).

A rule-based approach is used to define the causation relationships and influential magnitudes among all the nodes in BN. The approach describes causality between *IF* and *THEN* parts with several rules, which are used to convert p attendance attributes $\{A_1, A_2, \dots, A_p\}$ (*IF* part) into q states $\{C_1, C_2, \dots, C_q\}$ (*THEN* part) by assigning a belief degree β_s ($s = 1, 2, \dots, q$) to C_s ($s \in q$) ([48], [50]). For example, the w^{th} conventional *IF-THEN* rule R_w in a rule-based set can be expressed as:

$$R_w: \text{IF } A_1^w \text{ and } A_2^w \text{ and } \dots \text{ and } A_p^w, \text{ THEN } \{(\beta_1^w, C_1), (\beta_2^w, C_2), \dots, (\beta_q^w, C_q)\}.$$

In the w^{th} rule of R_w , the *IF* part is a set of linguistic inputs $A^w = \{A_1^w, A_2^w, \dots, A_p^w\}$. Under this situation, a set of belief degrees is assigned to the *THEN* part as $\{(\beta_1^w, C_1), (\beta_2^w, C_2), \dots, (\beta_q^w, C_q)\}$ for the description of how each C_s ($s = 1, 2, \dots, q$) is believed to be the result of β_s in the R_w , in which the β_s can be assigned with experience or by using converting methods (e.g. equivalent influential method [48]). Combining all rules of R , a multiple-input and multiple-output rule-based set can be developed. When conducting the *IF-THEN* rules, this research applies belief structures that helps us to identify the respondents' knowledge to the specific hazards. The rules with belief structures in FMEA can be established on the basis of expert judgments. Table 5 shows the 125 rules ($5 \times 5 \times 5$) with a rational DoB distribution.

Table 5 The established FRB with a belief structure

| Rule No | Parameters in the IF part | | | DoB in the THEN part | | | | |
|---------|---------------------------|-------------------|--------------------|----------------------|------|------|------|------|
| | L | C | P | R1 | R2 | R3 | R4 | R5 |
| 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 |

Use the above introduced approach, several rules are used in the MASS risk model and its sub-model of FMEA based BN. For instance, an *IF-THEN* rule to describe the relationship among L, C and P in the FMEA based BN is defined as follows:

Rule 1: IF the threat is determined as very low in likelihood (L1), and negligible in consequence (C1), and very unlikely in probability of the failure being undetected (P1),
THEN $\{(1, \text{very low (R1)}), (0, \text{low (R2)}), (0, \text{average (R3)}), (0, \text{high (R4)}), (0, \text{very high (R5)})\}$.

Rule 2: IF very low (L1), and negligible (C1), and unlikely (P2),
THEN $\{(0.67, \text{very low (R1)}), (0.33, \text{low (R2)}), (0, \text{average (R3)}), (0, \text{high (R4)}), (0, \text{very high (R5)})\}$.

The above two rules can be further explained as follows:

Rule 1: if the threat's L is very low, C is negligible, and P is very unlikely, then R 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.

Rule 2: if L is very low, C is negligible, and P is unlikely, then R 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: Rule aggregation using a Bayesian Reasoning mechanism

The observation information (e.g. expert judgements) 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 for each node is then developed by converting the IF-THEN rules into a conditional probability table. For example, the conditional probability table for the risk in the sub-FMEA based BN is given in Table 6.

Table 6 The conditional probability table (CPT) for the risk in the sub-FMEA based BN

| L | L1 | | | | | | L5 | | | | | |
|----|----|-----|------|------|-----|------|------|--|------|------|-----|----|
| C | C1 | | | C5 | | | C1 | | | C5 | | |
| P | P1 | | P5 | P1 | | P5 | P1 | | P5 | P1 | | P5 |
| R1 | 1 | | 0.67 | 0.67 | | 0.33 | 0.67 | | 0.33 | 0.33 | | 0 |
| R2 | 0 | | 0 | 0 | | 0 | 0 | | 0 | 0 | | 0 |
| R3 | 0 | ... | 0 | 0 | ... | 0 | 0 | | 0 | 0 | ... | 0 |
| R4 | 0 | | 0 | 0 | | 0 | 0 | | 0 | 0 | | 0 |
| R5 | 0 | | 0.33 | 0.33 | | 0.67 | 0.33 | | 0.67 | 0.67 | | 1 |

In Table 5, the first rule can be expressed as follows:

R₁: IF the threat has very low likelihood, negligible consequence and very unlikely probability of the failure being undetected, THEN the risk value can be denoted as {(1, (R₁)), (0, (R₂)), (0, (R₃)), (0, (R₄)), (0, (R₅))}.

where represent a condition that if L1 and C1 and P1, the probability of R (DoB) is $p(R|L_1, C_1, P_1) = (1, 0, 0, 0, 0)$.

After the model is well developed, the prior probabilities, which is the observed information, are aggregated to produce the results (i.e. marginal probabilities). Having analysed all prior probabilities of nodes in the BN, the marginal probability $p(R_h)$ for the result can be calculated as follows:

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

Step 5: Convert the obtained results into crisp values by using utility functions

After obtaining a set of DoB numbers representing the severity of a threat, we will convert this set of DoB numbers into a crisp value to make it more straightforward. Utility values are assigned to all the nodes in the MASS risk model and its sub-FMEA based BN to represent the severity of threats from different prospects. Then, the utility values are combined in the overall risk to prioritise threats. For example, from low risk influence on high influence, the utility values assign to L, C and P are $U_{L1}=U_{C1}=U_{P1}=1$; $U_{L2}=U_{C2}=U_{P2}=2$, $U_{L3}=U_{C3}=U_{P3}=3$, $U_{L4}=U_{C4}=U_{P4}=4$ and $U_{L5}=U_{C5}=U_{P5}=5$. Under this basis, five IF-THEN rules in Table are used to combine the utility values for R, there are 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,

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

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

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

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

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

A utility function is used to calculate crisp values (CV) by using the assigned utility values for R, it is given in the follows:

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

where t is the number of the linguistic variables that a node has. $p(R_h)$ is the marginal probability to the that demonstrated from the BN. U_z ($z = R1, R2, R3, R4, R5$) is the synthesised utility value that assigned to R. Similar utility values are also assigned to all nodes of threats and threats categories to convert the obtained result into crisp values, which are used to compare their risk degrees.

3.2.3 Three-dimensional risk matrix

Risk map is a common method that provides an overview of the risk scales by multiplying risk likelihood and consequence ([52], [53]). A three-dimensional (3D) risk matrix will also be conducted through Minitab to present in a simple and common way of the results to the maritime industry. Four categories are identified as “extreme” (highlighted as red colour, risk value more than 50), “high” (highlighted as orange colour, risk value between 40 and 49), “medium” (highlighted as yellow colour, risk value between 30 and 39) and “low” (highlighted as green colour, risk value lower than 29) to present the level of risk in maritime cybersecurity. Figure 7 is an example to presents 3D risk matrix structure.

The overall flowchart of the methodology is presented in Figure 8, which includes six tasks and the relevant methods to complete the task.

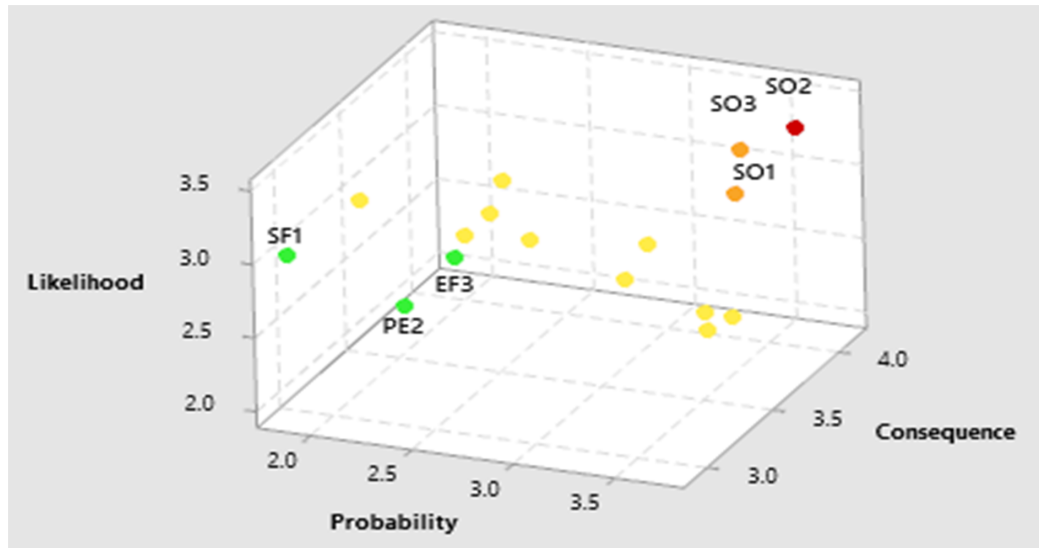


Fig. 7 Example of 3D risk matrix

Source: [51]

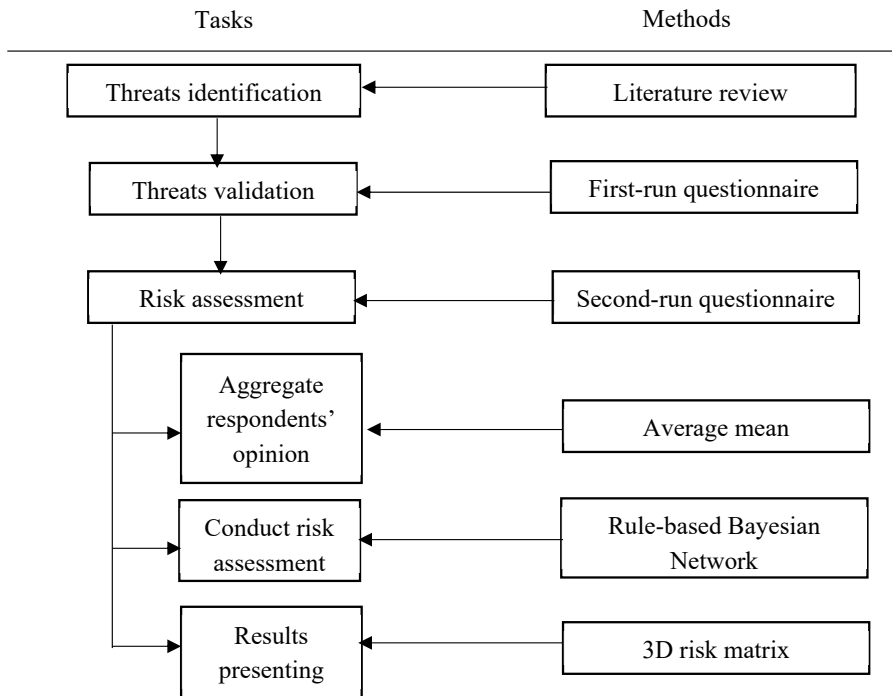


Fig. 8 *Flowchart of the methodology*

4. Research findings

4.1 Research findings on the first run questionnaire

Since we have identified a list of cyber threats, the purpose of the first run questionnaire (Appendix B) with Likert five-point scale is to validate the identified maritime cyber threats and to explore more if some threats are not identified from the literature review. select the relatively important cyber threats for further Bayesian Network analysis using the second questionnaire (Appendix C). In total, there were 31 replies from shipping companies, Capitan and sea crews, port authorities, IMO, and universities. The threshold of the selection for the next run is the mean value more than 3.2. In Table 7, threats with importance score lower than 3.2 (presented as *Italic*) will be removed; whereas the threats with importance score higher than 3.2 are retained for a further survey. The selected cyber threats and cyber threat categories can be seen in Table 9 or Appendix C.

Table 7 Results of expert judgement

| Rate | 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 | <i>Accessing links from impersonation text massage (e.g. bank, credit card company, insurance company, etc.)</i> |
| 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 | <i>Accessing malicious advertising on websites</i> |
| Man-in-the-middle-attack | |
| 2.67 | <i>Using unsecure open Wi-Fi connection</i> |
| 2.82 | <i>Using insecure Virtual Private Network (VPN)</i> |
| 2.67 | <i>Applying weak WEP/WPA encryption on access points</i> |
| 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) |
| Ransomware | |
| 3.61 | Accessing suspicious websites |
| 2.94 | <i>Downloading files from P2P site (e.g. torrent files, music, movies, etc.)</i> |
| 3.21 | <i>Downloading program from suspicious websites (e.g. illegal software/music/movie download websites)</i> |
| 2.94 | <i>Controlled computer by attacker through remote desktop protocol(RDP)</i> |
| 3.82 | Connecting your infected USB or removable media to connect computers/navigation systems |
| Theft of credentials | |
| 3.48 | Using automatically log in system (e.g. save your ID and password on website) |
| 3.58 | Using simple and easy to assume password |
| 3.33 | Applying only single factor authentication for log in account system |
| 3.24 | Providing personal information to a fake website (e.g. government website, etc.) |
| Distributed Denial of Service (DDoS/DoS) | |
| 3.03 | <i>DDoS attacks AIS database</i> |
| 2.85 | <i>DDoS attacks GPS and RADAR system</i> |
| 3.58 | DDoS attacks company's server system |

| Human error | |
|---------------------------------|--|
| 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 antivirus software |
| 3.70 | Using unpatched operating system e.g. outdated window version |
| 3.27 | Forgetting update software |
| 3.09 | <i>No planning applying up-to-date software</i> |

4.2 Research findings on Rule-based Bayesian Network

In order to have a better understanding on risk assessment of maritime cybersecurity, we selected 17 experts from shipping companies and research staff who have rich experience in the maritime industry and are familiar with the topic.

4.2.1 Respondents' background

For the second run questionnaire survey, in total there were 17 replies participated. The background of these 17 respondents including shipping companies, port authority, research institution, and the universities. All respondents have some experience related to maritime cybersecurity issues (e.g. training, faced cyberattacks before or other relevant experience). The details of their background are listed in Table 8.

Table 8 Respondents' background

| Respondent | Company type | Work experience |
|-------------------|----------------------|-------------------------|
| 1 | Shipping company | Less than 5 years |
| 2 | Shipping company | Less than 5 years |
| 3 | Shipping company | Less than 5 years |
| 4 | Shipping company | Less than 5 years |
| 5 | Shipping company | Less than 5 years |
| 6 | Shipping company | More than 16 years |
| 7 | Shipping company | Between 11 and 15 years |
| 8 | Shipping company | Between 6 and 10 years |
| 9 | Shipping company | More than 16 years |
| 10 | Research institution | Between 6 and 10 years |
| 11 | Port authority | Less than 5 years |
| 12 | University | Between 6 and 10 years |
| 13 | University | Between 11 and 15 years |
| 14 | Shipping company | Less than 5 years |
| 15 | University | More than 16 years |
| 16 | University | Less than 5 years |
| 17 | Shipping company | More than 16 years |

4.2.2 Research findings on the assessment of the 'Phishing' threat category

The results show that two threats are selected under the category of phishing based on the results of the interview, including 'Accessing links from impersonation emails (e.g. bank, credit card company, insurance company, etc.)' (Link from email in Fig. 9), and 'Downloading attached files from impersonation emails (e.g. bank, credit card company, insurance company, etc.)' (File from email in Fig. 9).

The results also show that the value of likelihood of 'Accessing links from impersonation emails (e.g. bank, credit card company, insurance company, etc.)' is around 2.63, with 9% of Very High (VH), 20% of High (H), 24% of Average (A), 16% of Low (L), and 30% of Very Low (VL). Whereas the value of consequence is around 3.61, with 21% of Catastrophic (CA), 36% of Critical (CR), 29% of Moderate (MO), 11% of Marginal (MA), and 3% of Negligible (N). For the value of Probability of the failure being undetected is around 2.9, with 11% of Highly likely (HL), 22% of Likely (L), 35% of Average (A), 12% of Unlikely (U), and 21% 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 43.30 after conducting BN calculation.

For the results of 'Downloading attached files from impersonation emails (e.g. bank, credit card company, insurance company, etc.)', the likelihood is around 2.54, with 5% of Very High (VH), 26% of High (H), 17% of Average (A), 24% of Low (L), and 29% of Very Low (VL). Whereas the value of consequence is around 3.58, with 22% of Catastrophic (CA), 36% of Critical (CR), 29% of Moderate (MO), 4% of Marginal (MA), and 9% of Negligible (N). For the value of Probability of the failure being undetected is around 2.84, with 7% of Highly likely (HL), 22% of Likely (L), 39% of Average (A), 10% of Unlikely (U), and 21% 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 41.82 after conducting BN calculation. Finally, the overall risk value of 'Phishing' is 42.56.

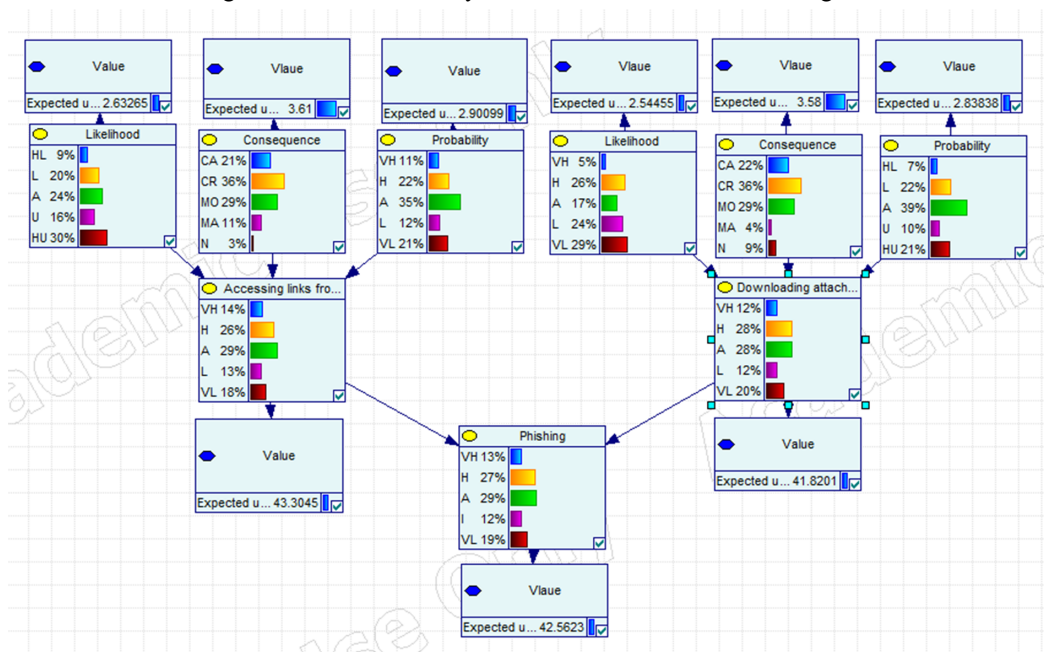


Fig. 9 Result of the assessment of the 'Phishing' threat category

4.2.3 Research findings on the assessment of the 'Malware' threat category

The results show that three threats are selected under the category of malware based on the results of the interview, including 'Accessing links from suspicious emails' (email link in Fig. 10), 'Downloading attached files from unknown emails' (email file in Fig. 10), and 'Connecting USB or removable media to computer without virus check' (USB in Fig. 10).

The results also show that the value of likelihood of 'Accessing links from suspicious emails' is around 2.79, with 14% of Very High (VH), 25% of High (H), 17% of Average (A), 14% of Low (L), and 30% of Very Low (VL). Whereas the value of consequence is around 3.28, with 13% of Catastrophic (CA), 29% of Critical (CR), 38% of Moderate (MO), 11% of Marginal (MA), and 8% of Negligible (N). For the value of Probability of the failure being undetected is around 2.66, with 8% of Highly likely (HL), 16% of Likely (L), 33% of Average (A), 20% of Unlikely (U), and 23% of Highly Unlikely (HU). The overall risk value for 'Accessing links from suspicious emails' is around 39.59 after conducting BN calculation.

For the results of 'Downloading attached files from unknown emails', the likelihood is around 2.63, with 10% of Very High (VH), 22% of High (H), 24% of Average (A), 11% of Low (L), and 34% of Very Low (VL). Whereas the value of consequence is around 3.38, with 15% of Catastrophic (CA), 39% of Critical (CR), 24% of Moderate (MO), 13% of Marginal (MA), and 9% of Negligible (N). For the value of Probability of the failure being undetected is around 2.54, with 4% of Highly likely (HL), 18% of Likely (L), 34% of Average (A), 16% of Unlikely (U), and 28% of Highly Unlikely (HU). The overall risk value for 'Downloading attached files from unknown emails' is around 37.9 after conducting BN calculation.

For the results of 'Connecting USB or removable media to computer without virus check', the likelihood is around 2.88, with 14% of Very High (VH), 20% of High (H), 17% of Average (A), 38% of Low (L), and 11% of Very Low (VL). Whereas the value of consequence is around 3.18, with 16% of Catastrophic (CA), 39% of Critical (CR), 9% of Moderate (MO), 17% of Marginal (MA), and 18% of Negligible (N). For the value of Probability of the failure being undetected is around 2.46, with 6% of Highly likely (HL), 11% of Likely (L), 26% of Average (A), 37% of Unlikely (U), and 20% of Highly Unlikely (HU). The overall risk value for 'Connecting USB or removable media to computer without virus check' is around 38.08 after conducting BN calculation. Finally, the overall risk value of 'Malware' is 38.76.

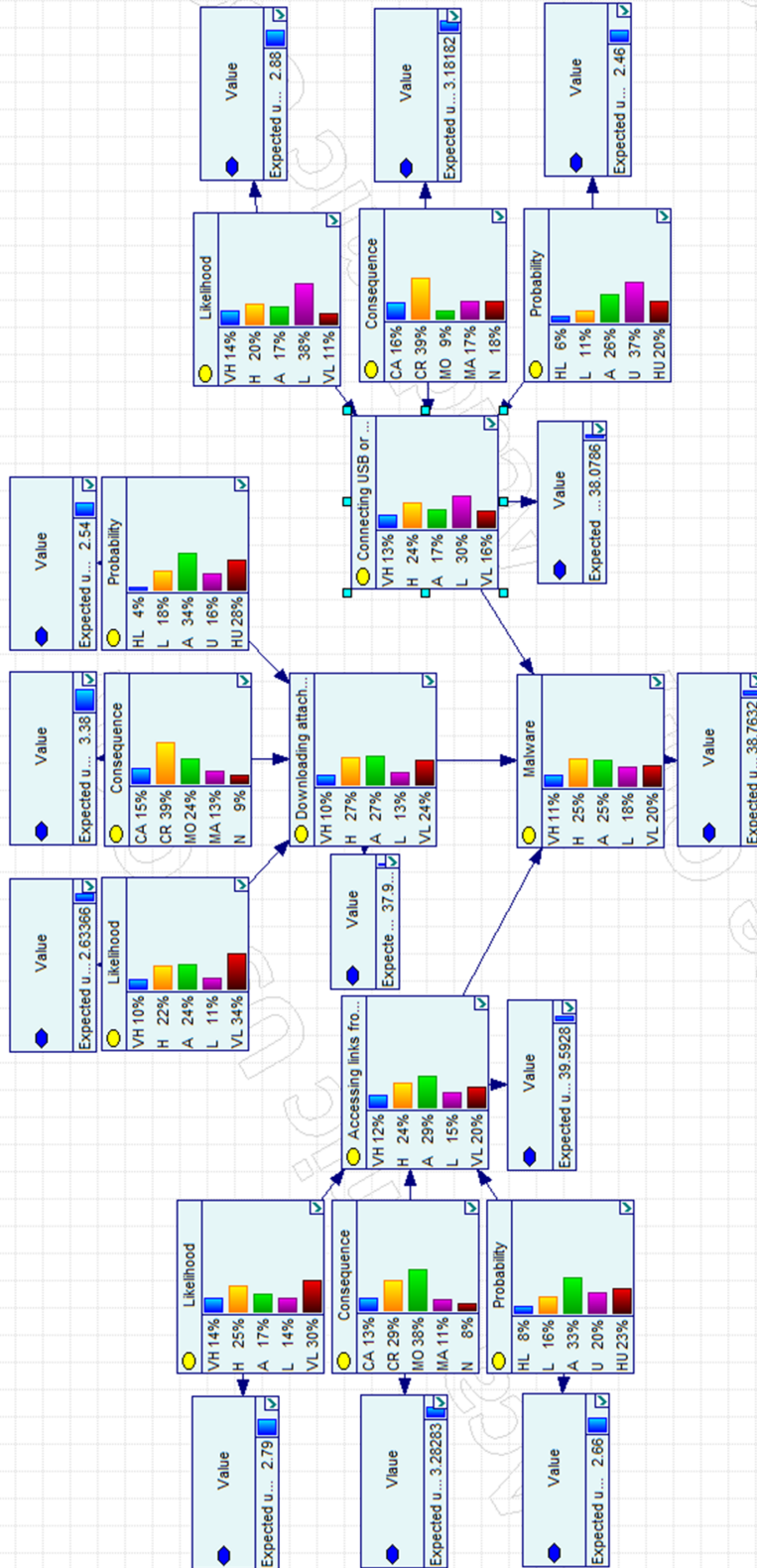


Fig. 10 Result of the assessment of the 'Malware' threat category

4.2.4 Research findings on the assessment of the ‘Man-in-the-middle’ threat category

The results show that two threats are selected under the category of Man-in-the-middle attack based on the results of the interview, including ‘Providing personal/commercial information to friends/partners via open Wi-Fi connection’ (open WiFi in Fig. 11), and ‘Providing personal/commercial information to suspicious websites (e.g. illegal software/music/movie download websites)’ (Suspicious websites in Fig. 11).

The results also show that the value of likelihood of ‘Providing personal/commercial information to friends/partners via open Wi-Fi connection’ is around 2.74, with 7% of Very High (VH), 22% of High (H), 30% of Average (A), 20% of Low (L), and 21% of Very Low (VL). Whereas the value of consequence is around 2.22, with 1% of Catastrophic (CA), 14% of Critical (CR), 26% of Moderate (MO), 24% of Marginal (MA), and 35% of Negligible (N). For the value of Probability of the failure being undetected is around 2.66, with 11% of Highly likely (HL), 9% of Likely (L), 32% of Average (A), 33% of Unlikely (U), and 16% of Highly Unlikely (HU). The overall risk value for ‘Providing personal/commercial information to friends/partners via open Wi-Fi connection’ is around 27.99 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 2.19, with 11% of Very High (VH), 11% of High (H), 15% of Average (A), 12% of Low (L), and 51% of Very Low (VL). Whereas the value of consequence is around 2.70, with 2% of Catastrophic (CA), 21% of Critical (CR), 39% of Moderate (MO), 19% of Marginal (MA), and 18% of Negligible (N). For the value of Probability of the failure being undetected is around 2.59, with 3% of Highly likely (HL), 18% of Likely (L), 34% of Average (A), 27% of Unlikely (U), and 19% 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 27.64 after conducting BN calculation. Finally, the overall risk value of ‘Man-in-the-middle’ is 27.82.

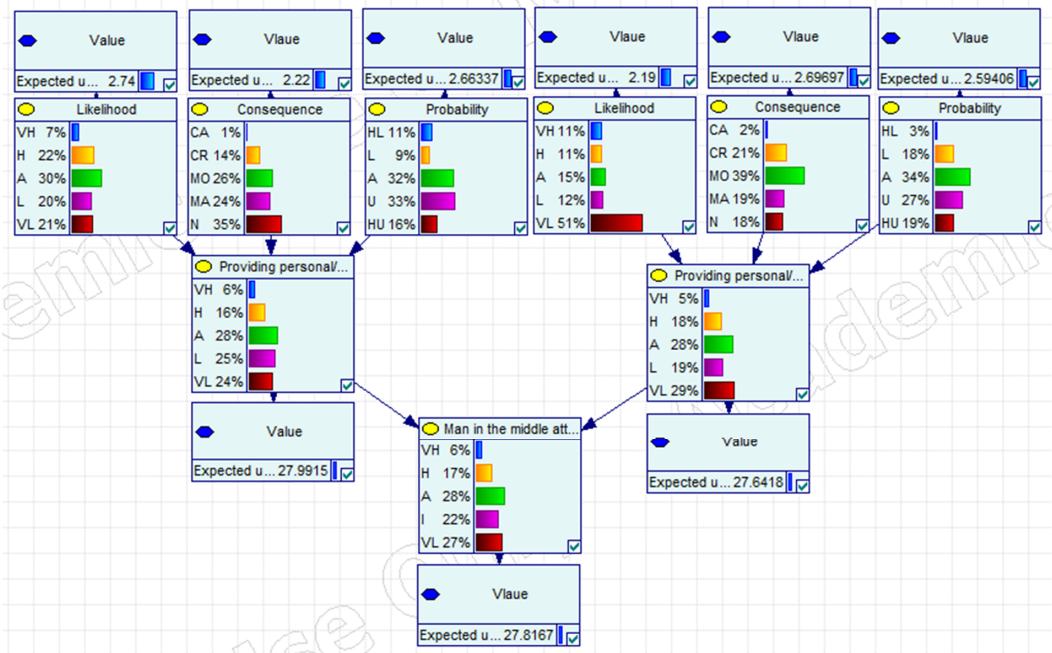


Fig. 11 Result of the assessment of the ‘Man-in-the-middle’ threat category

4.2.5 Research findings on the assessment of the 'Ransomware' threat category

The results show that two threats are selected under the category of ransomware based on the results of the interview, including 'Accessing suspicious websites' (Suspicious websites in Fig. 12), and 'Connecting your infected USB or removable media to connect computers/navigation systems' (Infected USB in Fig. 12).

The results also show that the value of likelihood of 'Accessing suspicious websites' is around 2.53, with 10% of Very High (VH), 18% of High (H), 18% of Average (A), 23% of Low (L), and 31% of Very Low (VL). Whereas the value of consequence is around 3.23, with 15% of Catastrophic (CA), 24% of Critical (CR), 37% of Moderate (MO), 17% of Marginal (MA), and 7% of Negligible (N). For the value of Probability of the failure being undetected is around 2.61, with 2% of Highly likely (HL), 16% of Likely (L), 36% of Average (A), 33% of Unlikely (U), and 13% of Highly Unlikely (HU). The overall risk value for 'Accessing suspicious websites' is around 34.35 after conducting BN calculation.

For the results of 'Connecting your infected USB or removable media to connect computers/navigation systems', the likelihood is around 2.82, with 17% of Very High (VH), 15% of High (H), 25% of Average (A), 19% of Low (L), and 24% of Very Low (VL). Whereas the value of consequence is around 3.10, with 13% of Catastrophic (CA), 20% of Critical (CR), 41% of Moderate (MO), 18% of Marginal (MA), and 9% of Negligible (N). For the value of Probability of the failure being undetected is around 2.74, with 7% of Highly likely (HL), 19% of Likely (L), 31% of Average (A), 27% of Unlikely (U), and 16% of Highly Unlikely (HU). The overall risk value for 'Connecting your infected USB or removable media to connect computers/navigation systems' is around 37.74 after conducting BN calculation. Finally, the overall risk value of 'Ransomware' is 36.05.

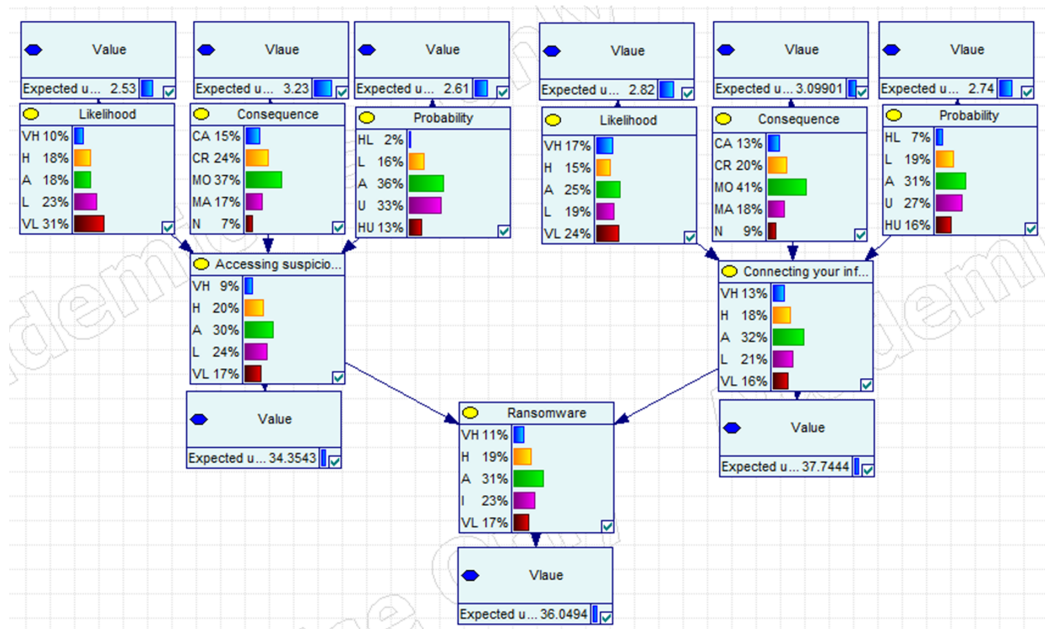


Fig. 12 Result of the assessment of the 'Ransomware' threat category

4.2.6 Research findings on the assessment of the 'Theft of credential' threat category

The results show that four threats are selected under the category of Theft of credential based on the results of the interview, including 'Using automatically log in system (e.g. save your ID and password on website)' (save password in Fig. 13), 'Using simple and easy to assume password' (easy password in Fig. 13), 'Applying only single factor authentication for log in account system' (single factor in Fig. 13), and 'Providing personal information to a fake website (e.g. government website, etc.)' (fake website in Fig. 13).

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 3.05, with 18% of Very High (VH), 24% of High (H), 26% of Average (A), 9% of Low (L), and 23% of Very Low (VL). Whereas the value of consequence is around 2.60, with 5% of Catastrophic (CA), 27% of Critical (CR), 16% of Moderate (MO), 25% of Marginal (MA), and 26% of Negligible (N). For the value of Probability of the failure being undetected is around 2.79, with 11% of Highly likely (HL), 17% of Likely (L), 29% of Average (A), 28% of Unlikely (U), and 16% 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 37.74 after conducting BN calculation.

For the results of 'Using simple and easy to assume password', the likelihood is around 2.93, with 12% of Very High (VH), 32% of High (H), 20% of Average (A), 9% of Low (L), and 27% of Very Low (VL). Whereas the value of consequence is around 2.64, with 6% of Catastrophic (CA), 22% of Critical (CR), 25% of Moderate (MO), 22% of Marginal (MA), and 24% of Negligible (N). For the value of Probability of the failure being undetected is around 2.77, with 11% of Highly likely (HL), 15% of Likely (L), 26% of Average (A), 34% of Unlikely (U), and 13% of Highly Unlikely (HU). The overall risk value for 'Using simple and easy to assume password' is around 35.67 after conducting BN calculation.

For the results of 'Applying only single factor authentication for log in account system', the likelihood is around 2.79, with 19% of Very High (VH), 8% of High (H), 29% of Average (A), 21% of Low (L), and 23% of Very Low (VL). Whereas the value of consequence is around 2.60, with 2% of Catastrophic (CA), 16% of Critical (CR), 41% of Moderate (MO), 22% of Marginal (MA), and 19% of Negligible (N). For the value of Probability of the failure being undetected is around 2.29, with 8% of Highly likely (HL), 6% of Likely (L), 32% of Average (A), 14% of Unlikely (U), and 39% of Highly Unlikely (HU). The overall risk value for 'Applying only single factor authentication for log in account system' is around 31.25 after conducting BN calculation.

For the results of 'Providing personal information to a fake website (e.g. government website, etc.)', the likelihood is around 2.29, with 8% of Very High (VH), 6% of High (H), 32% of Average (A), 14% of Low (L), and 39% of Very Low (VL). Whereas the value of consequence is around 3.03, with 12% of Catastrophic (CA), 25% of Critical (CR), 34% of Moderate (MO), 12% of Marginal (MA), and 17% of Negligible (N). For the value of Probability of the failure being undetected is around 2.62, with 4% of Highly likely (HL), 15% of Likely (L), 39% of Average (A), 23% of Unlikely (U), and 19% of Highly Unlikely (HU). The overall risk value for 'Providing personal information to a fake website (e.g. government website, etc.)' is around 31.25 after conducting BN calculation. Finally, the overall risk value of 'Theft of credential' is 34.40.

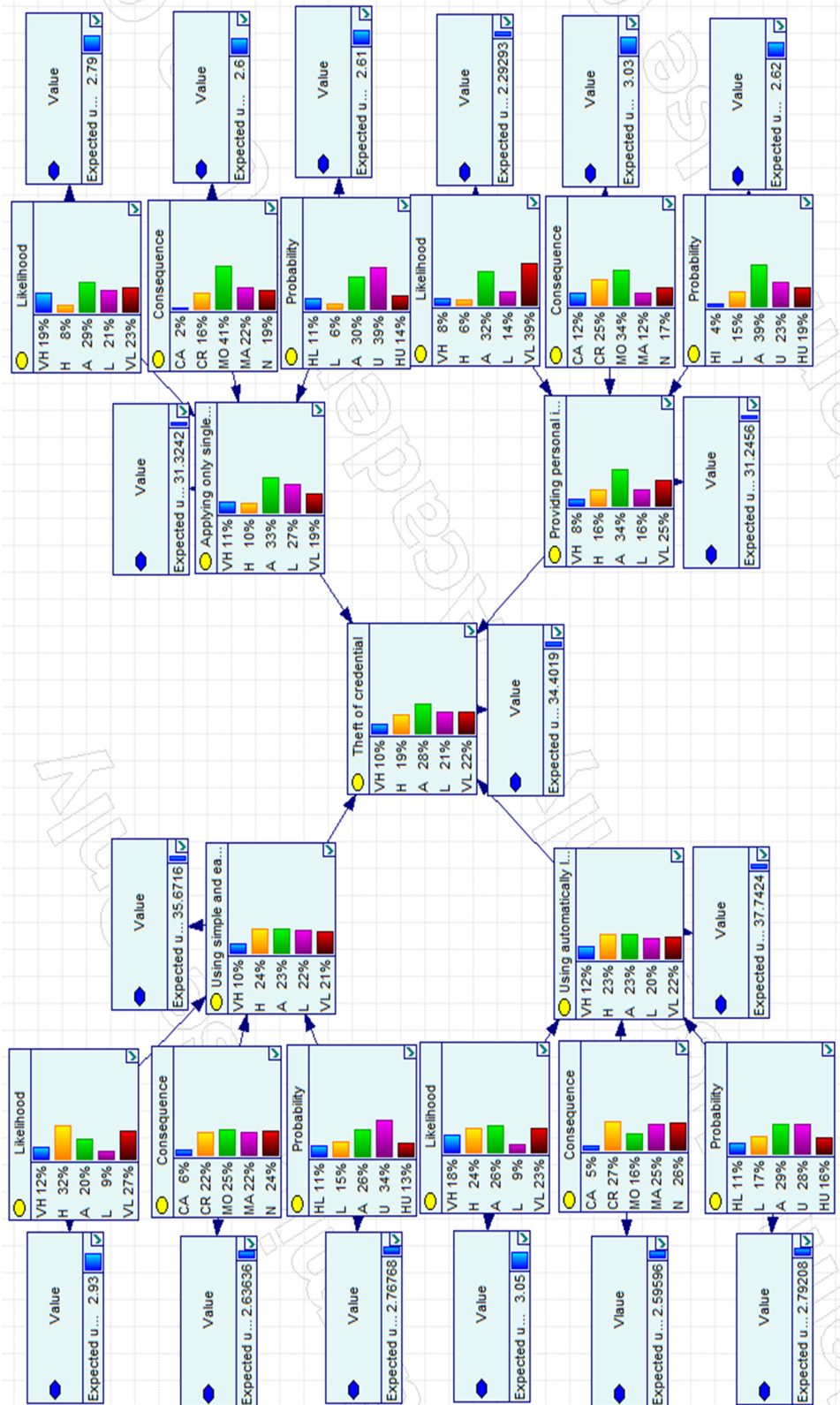


Fig. 13 Result of the assessment of the 'Theft of credential' threat category

4.2.7 Research findings on the assessment of the 'DDoS' threat category

The results show that only one threat is selected under the category of DDoS based on the results of the interview, which is 'DDoS attacks company's server system' (DDoS in Fig. 14).

The results also show that the value of likelihood of 'DDoS' is around 2.38, with 5% of Very High (VH), 8% of High (H), 34% of Average (A), 25% of Low (L), and 27% of Very Low (VL). Whereas the value of consequence is around 3.36, with 7% of Catastrophic (CA), 46% of Critical (CR), 31% of Moderate (MO), 8% of Marginal (MA), and 8% of Negligible (N). For the value of Probability of the failure being undetected is around 2.78, with 2% of Highly likely (HL), 22% of Likely (L), 42% of Average (A), 20% of Unlikely (U), and 14% of Highly Unlikely (HU). The overall risk value for 'DDoS' is around 34.42 after conducting BN calculation.

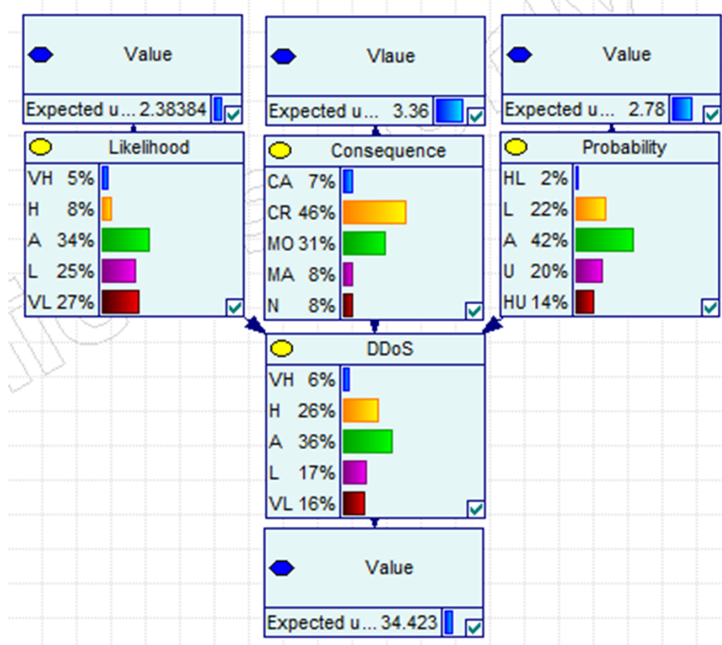


Fig. 14 Result of the assessment of the 'DDoS' threat category

4.2.8 Research findings on the assessment of the 'Human error' threat category

The results show that five threats are selected under the category of human error based on the results of the interview, including 'Lacking knowledge of cybersecurity (i.e. facing a new situation and do not know how to deal with it)' (Lack knowledge in Fig. 15), 'Company does not set a proper cybersecurity process' (Poor process in Fig. 15), 'Employees do not follow company's cybersecurity process due to poor cybersecurity awareness' (Poor awareness in Fig. 15), 'Closing firewall due to careless operations or specific purpose' (Close firewall in Fig. 15), and 'Accessing suspicious links due to careless operations or specific purpose' (Access link in Fig. 15).

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 3.03, with 16% of Very High (VH), 21% of High (H), 27% of Average (A), 22% of Low (L), and 14% of Very Low (VL). Whereas the value of consequence is around 2.68, with 6% of Catastrophic (CA), 22% of Critical (CR), 25% of Moderate (MO), 28% of Marginal (MA), and 19% of Negligible (N). For the value of Probability of the failure

being undetected is around 3.09, with 23% of Highly likely (HL), 14% of Likely (L), 29% of Average (A), 19% of Unlikely (U), and 16% 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 40.47 after conducting BN calculation.

For the results of 'Company does not set a proper cybersecurity process', the likelihood is around 2.13, with 5% of Very High (VH), 9% of High (H), 12% of Average (A), 41% of Low (L), and 32% of Very Low (VL). Whereas the value of consequence is around 2.99, with 12% of Catastrophic (CA), 31% of Critical (CR), 21% of Moderate (MO), 16% of Marginal (MA), and 20% of Negligible (N). For the value of Probability of the failure being undetected is around 2.49, with 4% of Highly likely (HL), 13% of Likely (L), 40% of Average (A), 14% of Unlikely (U), and 29% of Highly Unlikely (HU). The overall risk value for 'Company does not set a proper cybersecurity process' is around 29.80 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 2.76, with 13% of Very High (VH), 18% of High (H), 26% of Average (A), 18% of Low (L), and 25% of Very Low (VL). Whereas the value of consequence is around 2.9, with 6% of Catastrophic (CA), 29% of Critical (CR), 28% of Moderate (MO), 23% of Marginal (MA), and 14% of Negligible (N). For the value of Probability of the failure being undetected is around 2.86, with 14% of Highly likely (HL), 11% of Likely (L), 39% of Average (A), 19% of Unlikely (U), and 17% of Highly Unlikely (HU). The overall risk value for 'Employees do not follow company's cybersecurity process due to poor cybersecurity awareness' is around 36.66 after conducting BN calculation.

For the results of 'Closing firewall due to careless operations or specific purpose', the likelihood is around 2.65, with 15% of Very High (VH), 14% of High (H), 21% of Average (A), 21% of Low (L), and 29% of Very Low (VL). Whereas the value of consequence is around 2.85, with 6% of Catastrophic (CA), 28% of Critical (CR), 35% of Moderate (MO), 10% of Marginal (MA), and 22% of Negligible (N). For the value of Probability of the failure being undetected is around 2.66, with 11% of Highly likely (HL), 13% of Likely (L), 31% of Average (A), 23% of Unlikely (U), and 23% of Highly Unlikely (HU). The overall risk value for 'Closing firewall due to careless operations or specific purpose' is around 34.56 after conducting BN calculation.

For the results of 'Accessing suspicious links due to careless operations or specific purpose', the likelihood is around 2.35, with 6% of Very High (VH), 13% of High (H), 22% of Average (A), 27% of Low (L), and 31% of Very Low (VL). Whereas the value of consequence is around 3.06, with 6% of Catastrophic (CA), 31% of Critical (CR), 36% of Moderate (MO), 17% of Marginal (MA), and 10% of Negligible (N). For the value of Probability of the failure being undetected is around 2.66, with 5% of Highly likely (HL), 10% of Likely (L), 49% of Average (A), 18% of Unlikely (U), and 18% of Highly Unlikely (HU). The overall risk value for 'Accessing suspicious links due to careless operations or specific purpose' is around 30.67 after conducting BN calculation. Finally, the overall risk value of 'Human error' is 34.60.

4.2.9 Research findings on the assessment of the 'Using outdated IT' threat category

The results show that three threats are selected under the category of Using outdated IT based on the results of the interview, including 'Using outdated version firewall and antivirus software' (outdated firewall in Fig. 16), 'Using unpatched operating system e.g. outdated window version' (unpatched OS in Fig. 16), and 'Forgetting update software' (Outdated software in Fig. 16).

The results also show that the value of likelihood of 'Using outdated version firewall and antivirus software' is around 2.17, with 6% of Very High (VH), 9% of High (H), 19% of Average (A), 29% of Low (L), and 38% of Very Low (VL). Whereas the value of consequence is around 2.98, with 9% of Catastrophic (CA), 26% of Critical (CR), 34% of Moderate (MO), 16% of Marginal (MA), and 15% of Negligible (N). For the value of Probability of the failure being undetected is around 2.40, with 4% of Highly likely (HL), 12% of Likely (L), 28% of Average (A), 33% of Unlikely (U), and 24% of Highly Unlikely (HU). The overall risk value for 'Using outdated version firewall and antivirus software' is around 27.78 after conducting BN calculation.

For the results of 'Using unpatched operating system e.g. outdated window version', the likelihood is around 2.11, with 11% of Very High (VH), 6% of High (H), 15% of Average (A), 19% of Low (L), and 49% of Very Low (VL). Whereas the value of consequence is around 2.46, with 4% of Catastrophic (CA), 14% of Critical (CR), 32% of Moderate (MO), 24% of Marginal (MA), and 26% of Negligible (N). For the value of Probability of the failure being undetected is around 2.34, with 9% of Highly likely (HL), 5% of Likely (L), 24% of Average (A), 35% of Unlikely (U), and 27% of Highly Unlikely (HU). The overall risk value for 'Using unpatched operating system e.g. outdated window version' is around 24.54 after conducting BN calculation.

For the results of 'Forgetting update software', the likelihood is around 2.14, with 4% of Very High (VH), 7% of High (H), 31% of Average (A), 16% of Low (L), and 43% of Very Low (VL). Whereas the value of consequence is around 2.41, with 4% of Catastrophic (CA), 16% of Critical (CR), 26% of Moderate (MO), 24% of Marginal (MA), and 29% of Negligible (N). For the value of Probability of the failure being undetected is around 2.18, with 3% of Highly likely (HL), 5% of Likely (L), 28% of Average (A), 35% of Unlikely (U), and 29% of Highly Unlikely (HU). The overall risk value for 'Forgetting update software' is around 21.02 after conducting BN calculation. Finally, the overall risk value of 'Using outdated IT' is 24.41.

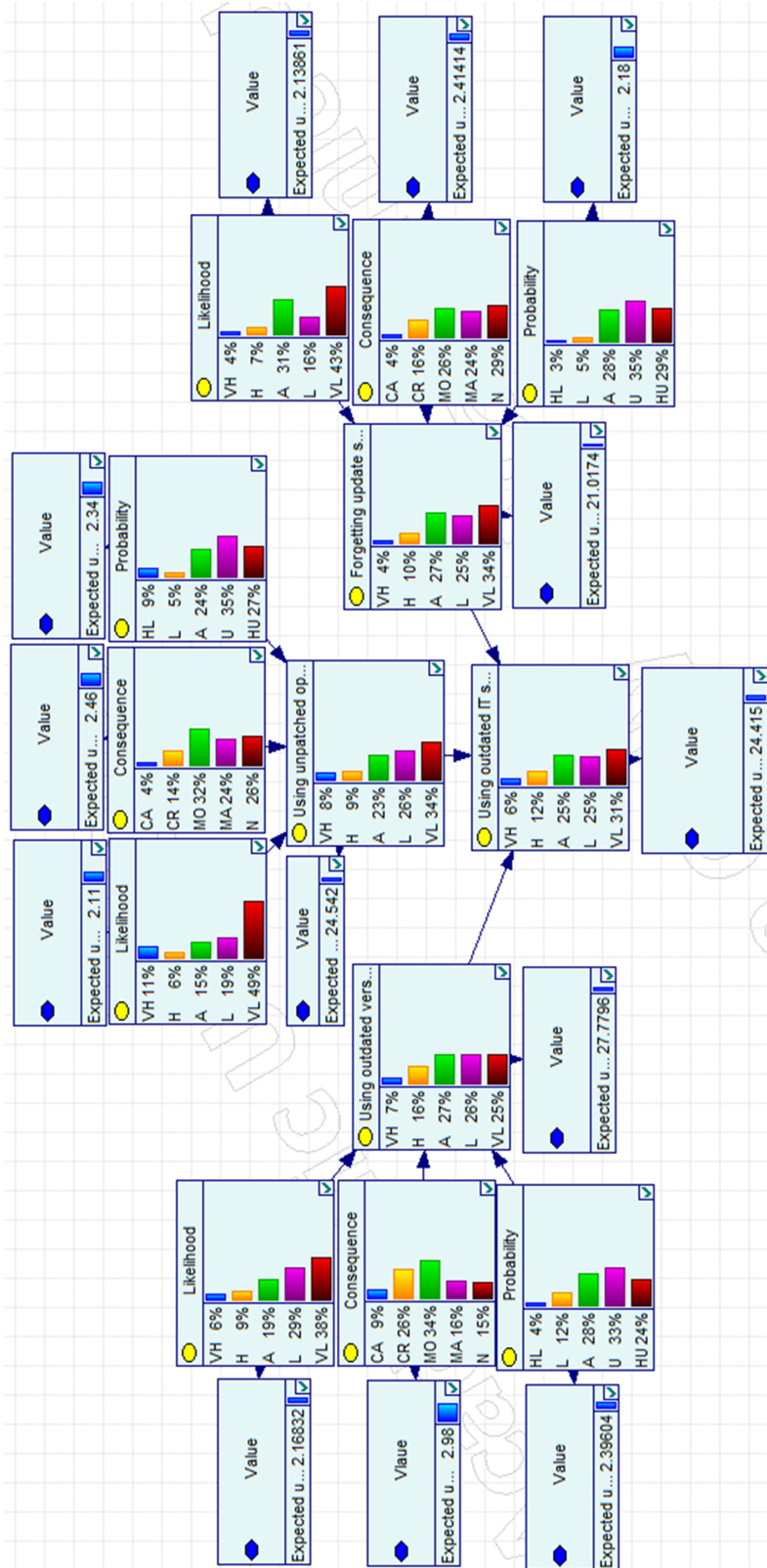


Fig. 16 Result of the assessment of the 'Using outdated IT' threat category

4.2.10 Summary of the risk values of maritime cyber threat categories and threats

The summarise the risk value of each threat category and hazard to MASS operations in Table 9. We use orange colour to present the risk value with higher than 40, yellow colour to present risk value between 30 and 40, and green colour to present risk value less than 30. The results show that ‘Phishing’ is the threat category with highest risk value of 42.56, following by ‘Malware’ (risk value: 38.76), and ‘Ransomware’ (risk value: 36.05); whereas the less important threat category contributes to maritime cybersecurity risk is ‘Outdated IT’ (risk value: 24.41). Apart from that, two of top three threats are belong to ‘Phishing’, including ‘Accessing links from impersonation emails (e.g. bank, credit card company, insurance company, etc.)’ (risk value: 43.30), ‘Downloading attached files from impersonation emails (e.g. bank, credit card company, insurance company, etc.)’ (risk value: 41.82), and one from ‘Human error’ called ‘Lacking knowledge of cybersecurity (i.e. facing a new situation and do not know how to deal with it)’ (risk value: 40.47); whereas the last three important threats contribute to maritime cybersecurity risk are all belong to ‘Using outdated IT’, including ‘Forgetting update software’ (risk value: 21.02), ‘Using unpatched operating system e.g. outdated window version’ (risk value: 24.54), and ‘Providing personal/commercial information to suspicious websites (e.g. illegal software/music/movie download websites)’ (risk value: 27.64).

Table 9 Risk values of threat categories and threats

| Threat category | Category value | Threat | Threat value |
|---------------------|----------------|--|--------------|
| Phishing | 42.56 | Accessing links from impersonation emails (e.g. bank, credit card company, insurance company, etc.) (Ph1) | 43.30 |
| | | Downloading attached files from impersonation emails (e.g. bank, credit card company, insurance company, etc.) (Ph2) | 41.82 |
| Malware | 38.76 | Accessing links from suspicious emails (Ma1) | 39.59 |
| | | Downloading attached files from unknown emails (Ma2) | 37.90 |
| | | Connecting USB or removable media to a computer without virus check (Ma3) | 38.08 |
| Men-in-the-middle | 27.82 | Providing personal/commercial information to friends/partners via open Wi-Fi connection (MITM1) | 27.99 |
| | | Providing personal/commercial information to suspicious websites (e.g. illegal software/music/movie download websites) (MITM2) | 27.64 |
| Ransomware | 36.05 | Accessing suspicious websites (Ra1) | 34.35 |
| | | Connecting your infected USB or removable media to connect computers/navigation systems (Ra2) | 37.74 |
| Theft of credential | 34.40 | Using automatically log in system (e.g. save your ID and password on website) (TC1) | 37.74 |
| | | Using simple and easy to assume password (TC2) | 35.67 |
| | | Applying only single factor authentication for login account system (TC3) | 31.32 |
| | | Providing personal information to a fake website (e.g. government website, etc.) (TC4) | 31.25 |
| DDoS | 34.42 | DDoS attacks company’s server system | 34.42 |
| Human error | 34.60 | Lacking knowledge of cybersecurity (i.e. facing a new situation and do not know how to deal with it) (HE1) | 40.47 |
| | | Company does not set a proper cybersecurity process (HE2) | 29.80 |
| | | Employees do not follow company’s cybersecurity process due to poor cybersecurity awareness (HE3) | 36.65 |

| Threat category | Category value | Threat | Threat value |
|-------------------|----------------|---|--------------|
| | | Closing firewall due to careless operations or specific purpose (HE4) | 34.56 |
| | | Accessing suspicious links due to careless operations or specific purpose (HE5) | 30.67 |
| Using outdated IT | 24.41 | Using outdated version firewall and antivirus software (IT1) | 27.78 |
| | | Using unpatched operating system e.g. outdated window version (IT2) | 24.54 |
| | | Forgetting update software (IT3) | 21.02 |

4.3 Research findings on 3D risk matrix

Table 10 summarises the three parameters (i.e. likelihood, consequence, and probability of the failure being undetected) of each maritime cyber threats, which can also be seen in Figure 9-16. Based on the three parameters, we further use a 3D risk matrix to illustrates the location of the maritime cyber threats (Figure 17). The same classification as Table 8, we use orange colour to present the risk value with higher than 40, yellow colour to present risk value between 30 and 40, and green colour to present risk value less than 30.

Table 10 Threats' likelihood, consequence, and probability of the failure being undetected

| Cyber threats | Likelihood | Consequence | Probability |
|--|------------|-------------|-------------|
| Accessing links from impersonation emails (e.g. bank, credit card company, insurance company, etc.) (Ph1) | 2.63 | 3.61 | 2.9 |
| Downloading attached files from impersonation emails (e.g. bank, credit card company, insurance company, etc.) (Ph2) | 2.54 | 3.58 | 2.84 |
| Accessing links from suspicious emails (Ma1) | 2.79 | 3.28 | 2.66 |
| Downloading attached files from unknown emails (Ma2) | 2.63 | 3.38 | 2.54 |
| Connecting USB or removable media to a computer without virus check (Ma3) | 2.88 | 3.18 | 2.46 |
| Providing personal/commercial information to friends/partners via open Wi-Fi connection (MITM1) | 2.74 | 2.22 | 2.66 |
| Providing personal/commercial information to suspicious websites (e.g. illegal software/music/movie download websites) (MITM2) | 2.19 | 2.7 | 2.59 |
| Accessing suspicious websites (Ra1) | 2.53 | 3.23 | 2.61 |
| Connecting your infected USB or removable media to connect computers/navigation systems (Ra2) | 2.82 | 3.1 | 2.74 |
| Using automatically log in system (e.g. save your ID and password on website) (TC1) | 3.05 | 2.6 | 2.79 |
| Using simple and easy to assume password (TC2) | 2.93 | 2.64 | 2.77 |
| Applying only single factor authentication for login account system (TC3) | 2.79 | 2.6 | 2.61 |
| Providing personal information to a fake website (e.g. government website, etc.) (TC4) | 2.29 | 3.03 | 2.62 |
| DDoS attacks company's server system | 2.38 | 3.36 | 2.78 |
| Lacking knowledge of cybersecurity (i.e. facing a new situation and do not know how to deal with it) (HE1) | 3.03 | 2.68 | 3.09 |
| Company does not set a proper cybersecurity process (HE2) | 2.13 | 2.99 | 2.49 |

| Cyber threats | Likelihood | Consequence | Probability |
|---|------------|-------------|-------------|
| Employees do not follow company's cybersecurity process due to poor cybersecurity awareness (HE3) | 2.76 | 2.9 | 2.86 |
| Closing firewall due to careless operations or specific purpose (HE4) | 2.65 | 2.85 | 2.66 |
| Accessing suspicious links due to careless operations or specific purpose (HE5) | 2.35 | 3.06 | 2.66 |
| Using outdated version firewall and antivirus software (IT1) | 2.17 | 2.98 | 2.4 |
| Using unpatched operating system e.g. outdated window version (IT2) | 2.11 | 2.46 | 2.34 |
| Forgetting update software (IT3) | 2.14 | 2.41 | 2.18 |

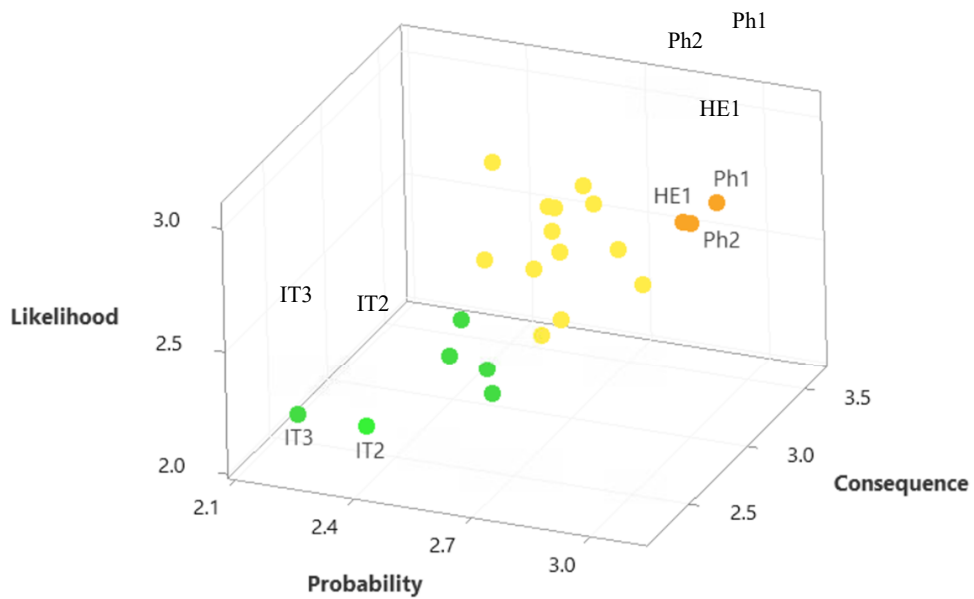


Fig. 17 Three-Dimensional scatterplot of maritime cyber threats

5. Discussion and conclusions

This project aims to conduct a risk assessment on maritime cybersecurity. A list of cyber threats and cyber threat categories are identified through a systematic literature review and validated by an expert (Objective 1). A first-run questionnaire is conducted to select the relatively important cyber threats under each cyber threat category. The results are designed for a second-run questionnaire with Likert five-point linguistic terms scale with BoD. A hybrid method combined FMEA and rule-based Bayesian network is applied to analyse the importance of the cyber threats and cyber threat categories to the context of maritime cybersecurity (Objective 2). In this report, the main contribution is the BN building and risk assessment part, as the proposed BN model can be further developed and expanded with other threats or categories from another perspectives (e.g. political issue, terrorism and piracy attacks, etc.). Finally, a list of risk control options for maritime cyber threats are provided (Objective 3).

The results show that the category of “Phishing” contributes the most to the maritime cybersecurity risk, with the category’s value more than 40. By checking the aggregated raw data, the consequence of the three parameters (i.e. likelihood, consequence, and probability of the threat been undetected) have the highest values. This indicates that the maritime industry should try to find some methods either to mitigate the impacts of the consequences once phishing happens or to prevent them happen from reducing the likelihood or probability of the threat been 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 on the maritime industry. On the other side, the lowest cyber threat category is “Using outdated IT” with a value lower than 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, we found that the likelihood of the three cyber threats are the lowest among the three parameters, which imply that most of the respondents believe that their companies have updated the IT to the latest version to protect the damage from the cyber-attacks.

From the cyber threat aspect, the most crucial one is ‘Accessing links from impersonation emails (e.g. bank, credit card company, insurance company, etc.)’, following by ‘Downloading attached files from impersonation emails (e.g. bank, credit card company, insurance company, etc.)’, and ‘Lacking knowledge of cybersecurity (i.e. facing a new situation and do not know how to deal with it) with threat values more than 40. Sea crews and company staffs 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 three cyber threats can all be avoided through high cybersecurity awareness, which is established by regular training and education.

Several research limitations happened when conducting this project. First, we have limited replies from the target sample for both the first-run and second-run questionnaires. This might due to the complicated questionnaires that are not easy to answer and our limited network. Although we have collected enough replies for the rule-based Bayesian network analysis, it will be, of cause, more reliable if we obtained more replies. In addition, the respondents’ background may be another factor that impacts on the reliability of the result. For instance, we have collected more than 20 replies for the second-run questionnaire, but only 17 replies can be used for further analysis after checking the answers they replied. Because of the COVID-19 pandemic, the second-run questionnaire cannot be checked right after they answered the questions, and some respondents did not reply after the first-attempt answering this questionnaire, which reduces the number of reliable replies. We will collect more replies (e.g. expand

the regions to other continents such as Asia and America) in the future to achieve acceptable replies numbers for further statistics analysis. Secondly, some respondents' work experiences are considered as junior (i.e. less than five years work experience), which is again due to our limited network. However, all respondents have some experience related to cybersecurity issues, although maritime cybersecurity is an emerging issue and everyone has different experience with such issue. Yet, the future research can conduct analysis with different weighting for people with different levels of familiarity to the maritime cybersecurity. In addition, from another angle, these group of respondents might be more sensible to the threats of cybersecurity as they might have more experience on using the internet. Although we do not collect enough replies for mean comparison analysis such as Analysis of variance (ANOVA) or t-test, the trend of the data shows the junior respondents have higher mean value in most of cyber threats compared to senior ones. This can be a notable insight for IAMU members, seafarers training institutes or company managers to pay more attention to enhance the cybersecurity awareness to the senior seafarers or staff. In addition, we are planning to submit a research proposal related to the maritime cybersecurity awareness to another research grant. The results are expected to provide some contribution to the academia and the industry. Moreover, as mentioned above, we will continue collecting the questionnaires to collect some respondents with senior work experience to enhance the reliable of the research. Thirdly, this research addresses maritime cyber threats more on human error and IT perspective. Although there were some operation technology (OT) items listed in the first-run questionnaire, their mean values are not higher than the threshold and thus are not listed in the second-run questionnaire. The second-run questionnaire is used to evaluate the cyber threats with three parameters (likelihood, consequence and probability of failure undetected), it will be more appropriate to list relative important threats based on the results of the first-run questionnaire to increase respondents' willingness answering the questionnaire. Apart from that, most of OT systems will transfer the signal to IT systems and thus the results can be deemed as a further risk assessment. However, the significant impact of OT system such as Global Positioning Systems (GPS), Automatic Identification Systems (AIS), and Electronic Chart Display and Information Systems (ECDIS) are also vulnerabilities to maritime cybersecurity and need to be considered as well. A list of OT systems can be found from Appendix A identified by DNV GL [59]. For the further research, it is suggested to address more on OT perspective to fill the gap. Fourthly, the consequence can be different types. In Bow-Tie method, the consequence can include people (safety), environment, asset, and reputation. In DNV GL report, they also provide several consequence types (see Appendix B in our report). In our research, the consequences are aggregated. For further research, there is a need to investigate the details of different consequence types to analyse the consequence from different aspects. In addition, because of time and cost limitation, we do not conduct the Bow-Tie method with a series of cybersecurity cases. However, we think the Bow-Tie method is an easy apply method that clearly illustrates how to deal with the identified cyber threats, which barriers can be used to mitigate the probability of the attack incidents from a certain threat, and if the incident happen then which barriers can largely reduce the negative impacts from such threat. For further research, it is suggested to apply relevant methods using a straightforward figure to illustrate the process of maritime cybersecurity.

Acknowledgement

We would like to thank International Association of Maritime Universities (IAMU) and the Nippon Foundation for the financial support to this project, and the reviewers' valuable comments.

References

- [1] UNCTAD, “Review of Maritime Transport 2019”, (2019). Available at: https://unctad.org/en/PublicationsLibrary/rmt2019_en.pdf
- [2] Nettitude, “The IMO Maritime Cyber Security Guidelines”, (2019). Available at: <https://blog.nettitude.com/the-new-imo-maritime-cyber-security-guidelines-nettitude>
- [3] Caponi, S., and Belmont, K., “Maritime cybersecurity: A growing threat goes unanswered”, *Intellectual Property and Technology Law Journal*, Vol. 27 No. 1, (2015), pp 16-18.
- [4] Gopalakrishnan, K., Govindarasu, M., Jacobson, D.W. and Phares, B.M., “Cyber security for airports”, *International Journal for Traffic and Transport Engineering*, Vol. 3 No. 4, (2013), pp 365-376.
- [5] Johnson, D.P., “Civil Aviation and Cyber Security”, (2013). Available at: http://sites.nationalacademies.org/cs/groups/depssite/documents/webpage/deps_084768.pdf
- [6] Suciu, G., Scheianu, A., Petre, I., Chiva, L. and Bosoc, C.S., “Cybersecurity Threats Analysis for Airports”. *Proc. World Conference on Information Systems and Technologies*, Springer, Cham, (2019), pp 252-262.
- [7] Coventry, L., & Branley, D., “Cybersecurity in healthcare: A narrative review of trends, threats and ways forward”, *Maturitas*, Vol. 113, (2018), pp 48-52.
- [8] Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., and Kusev, P., “Risk perceptions of cyber-security and precautionary behavior”, *Computers in Human Behavior*, Vol.75 No. 1, (2017), pp 547-559.
- [9] Ren, A., Wu, D., Zhang, W., Terpenney, J. and Liu, P., “Cyber security in smart manufacturing: survey and challenges”. *Proc. IIE Annual Conference*, Institute of Industrial and Systems Engineers (IISE), (2017), pp. 716-721.
- [10] Lezzi, M., Lazoi, M. and Corallo, A., “Cybersecurity for Industry 4.0 in the current literature: A reference framework”, *Computers in Industry*, Vol. 103, (2018), pp 97-110.
- [11] Bullock, J.A., Haddow, G.D. and Coppola, D.P., “Homeland security: the essentials”, 2nd edition. *Chapter 8 Cybersecurity and Critical Infrastructure Protection*, (2018), pp 189-226
- [12] BBC, “Police warning after drug traffickers' cyber-attack”, (2013). Available at: <https://www.bbc.co.uk/news/world-europe-24539417>
- [13] Wood, I. and Kim, S., “North Korea Jams GPS Signals to Fishing Boats: South”, (2016). Available at: <https://www.nbcnews.com/news/world/north-korea-jams-gps-signals-fishing-boats-south-n548986>
- [14] Novet, J., “Shipping company Maersk says June cyberattack could cost it up to \$300 million”, (2017). Available at: <https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html>
- [15] COSCO World Maritime News, “COSOCO shipping lines falls victim of cyberattack”, (2018). Available at: <https://worldmaritimeneeds.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/>
- [16] Information Security Newspaper, “Hacking attack in port of Barcelona”, (2018). Available at: <https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/>
- [17] BBC New, “San Diego port hit by ransomware attack”, (2018). Available at: <https://www.bbc.co.uk/news/technology-45677511>
- [18] Defense One, “Russia Launched Cyber Attacks Against Ukraine Before Ship Seizures, Firm Says”, (2018). Available at: <https://www.defenseone.com/technology/2018/12/russia-launched-cyber-attacks-against-ukraine-ship-seizures-firm-says/153375/>

- [19] Business Insider Australia, “A hacker broke into defense contractor Austal then made an extortion attempt”, (2018). Available at: <https://www.businessinsider.com.au/austal-hacked-extortion-defence-contractor-2018-11>
- [20] BC News, “China hackers steal data from US Navy contractor”, (2018). Available at: <https://www.bbc.co.uk/news/world-us-canada-44421785>
- [21] BANKINFOSECURITY, “Malware on the High Sea: US Coast Guard Issues Alert”, (2019). Available at: <https://www.bankinfosecurity.com/us-coast-guard-warns-maritime-malware-attacks-a-12759>
- [22] Schröder-Hinrichs, J. U., “Human and organizational factors in the maritime world—are we keeping up to speed?”, *WMU Journal of Maritime Affairs*, Vol. 9 No. 1, (2010), pp 1–3.
- [23] Heij, C. and Knapp, S, “Predictive power of inspection outcomes for future shipping accidents—an empirical appraisal with special attention for human factor aspects”, *Maritime Policy and Management*, Vol. 45 No. 5, (2018), pp 604-621.
- [24] North P&I Club, “Cyber risk in shipping”, North of England P&I group, (2017).
- [25] Sen, R., “Chapter 9. Cyber and information threats to seaports and ships.” *McNicholas, MA, Maritime Security*, Vol 2, (2016), pp 281- 302.
- [26] Jones, K. D., Tam, K., & Papadaki, M., “Threats and impacts in maritime cyber security”, *IET Engineering & Technology Reference*, (2016).
- [27] Teoh, C.S. and Mahmood, A.K., “Cybersecurity Workforce Development for Digital Economy”, *The Educational Review, USA*, Vol. 2 No. 1, (2018), pp.136-146.
- [28] BIMCO, “The Guidelines on Cyber Security Onboard Ships”, Vol. 3, (2018).
- [29] IMO, “Guidelines on Maritime Cyber Risk Management”, MSC-FAL.1/Circ.3REFERENCES, (2017).
- [30] Transport Canada, “Understanding cyber risk: best practice for Canada’s maritime sector”, (2016). Available at: <http://publications.gc.ca/site/fra/9.826132/publication.html>
- [31] IRCLASS Indian Register of Shipping, “Guidelines on Maritime Cyber Safety”, (2017). Available at: https://www.irclass.org/media/3635/guidelines-on-maritime-cyber-safety_1.pdf
- [32] Japan P&I Club, “Cyber risk and Cyber security countermeasures”, P&I Loss Prevention Bulletin, Vol 42, (2018), pp 2-14. Available at: <https://www.piclub.or.jp/wp-content/uploads/2018/05/Loss-Prevention-Bulletin-Vol.42-Full.pdf>
- [33] SECUREBOX, “Man In The Middle Attack (MitM)”, (2019). Available at: <https://securebox.comodo.com/ssl-sniffing/man-in-the-middle-attack/>
- [34] Svilicic, B., Kamahara, J., Rooks, M., and Yano, Y. “Maritime cyber risk management: an experimental ship assessment”, *The Journal of Navigation*, Vol. 72 No. 5, (2019), pp 1108-1120.
- [35] Fayi, S.Y.A., “What Petya/NotPetya ransomware is and what its remediations are”, *Proc. Information Technology-New Generations*, Springer, Cham, (2018), pp. 93-100,
- [36] McAfee Labs, “Threats Report”, May (2015).
- [37] Search Security, “Credential theft”, (2019). Available at: <https://searchsecurity.techtarget.com/definition/credential-theft>
- [38] Boyes, H., Isbell, R., and Luck, A., “Code of Practice-Cyber Security for Ships”, London, United Kingdom, (2017).
- [39] Lagouvardou, S., “Master thesis: Maritime Cyber Security: concepts, problems and models”, Technical University of Denmark – DNU, (2018). Available at: http://orbit.dtu.dk/files/156025857/Lagouvardou_MScThesis_FINAL.pdf
- [40] Bhasin, M., “Mitigating cyber threat to banking industry”, *The Chartered Accountant*, Vol. 50 No. 10, (2007), pp 1618-1624

- [41] CISCO, “Security priorities for IoT and connected healthcare”, (2018). Available at: https://www.cisco.com/c/dam/en_us/solutions/industries/healthcare/cic-briefing-note-security-priorities-for-health-us.pdf
- [42] Fitton, O., Prince, D., Germond, B., & Lacy, M., “The future of maritime cyber security”, (2015), Lancaster University.
- [43] Hiller, A.L., “The Challenge of Cybersecurity in the Maritime Domain”, (2017). Available at: <https://alexanderlhiller.wordpress.com/2017/05/11/the-challenge-of-cybersecurity-in-the-maritime-domain/>
- [44] National Cyber Security Centre, “Password managers: how they help you secure passwords”, London, United Kingdom, (2019). Available at: <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online?curPage=/collection/top-tips-for-staying-secure-online/password-managers>
- [45] Penttilä, O.J.J., “Cyber Threats in Maritime Container Terminal Automation Systems”, MSc. thesis, Tampere University of Technology, (2016).
- [46] VARONIS, “What is a Proxy Server and How Does it Work?”, (2019). Available at: <https://www.varonis.com/blog/what-is-a-proxy-server/>
- [47] Syngress Publishing, “Chapter 9. Microsoft Exchange Server 5.5, E-mail virus protection handbook”, (2000), pp 333-365.
- [48] Yang, Z.L., Bonsall, S. & Wang, J., “Fuzzy Rule-Based Bayesian Reasoning Approach for Prioritization of Failures in FMEA”, *IEEE Transactions on Reliability*, Vol. 57 No. 3, (2008), pp 517-528.
- [49] Liu, H. C., Liu, L., Bian, Q. H., Lin, Q. L., Dong, N., & Xu, P. C., “Failure mode and effects analysis using fuzzy evidential reasoning approach and grey theory”, *Expert Systems with Applications*, Vol. 38 No. 4, (2011), pp 4403-4415.
- [50] Yu Q., Liu K. Chang. C and Yang Z., “Realising advanced risk assessment of vessel traffic flows near offshore wind farms”, *Reliability Engineering & System Safety*, Vol. 203, (2020), 107086.
- [51] Chang, C.H., Kontovas, C. and Yang, X., “Risk evaluation of maritime autonomous surface ships in the UK”, Final report for the CILT Seed Corn fund, (2019)..
- [52] Chang, C.H., Xu, J., and Song, D.P., “An analysis of safety and security risks in container shipping operations: a case study of Taiwan”, *Safety Science*, Vol. 63, (2014), pp. 168-178.
- [53] Chang, C.H., Xu, J., and Song, D.P., “Risks Analysis in Container Shipping – from a logistics perspective”, *International Journal of Logistics Management*, Vol. 26 No. 1, (2015), pp.147-171.
- [54] Coventry, L., & Branley, D., “Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*”, Vol. 113, (2018), pp. 48-52.
- [55] Refsdal, A., Solhaug, B., & Stølen, K. Cyber-risk management. In *Cyber-Risk Management* (pp. 33-47). Springer, Cham. (2015).
- [56] Tam, K., & Jones, K. D. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, Vol. 3 No. 2, (2018), pp. 147-164.
- [57] Pajunen, N.. "Overview of Maritime Cybersecurity." (2017) Bachelor's Thesis, South-Eastern Finland University of Applied Sciences
- [58] Saunders, B. Maritime Cyber Security: Threats and Opportunities. NCC group (2015).
- [59] DNV GL. Cyber security resilience management for ships and mobile offshore units in operation. (2016)
- [60] IMO. Interim Guidelines on Maritime Cyber Risk Management: IMO-MSC 1/CIRC 1526 (2016)
- [61] Kessler, G. C., Craiger, J. P., & Haass, J. C. A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, Vol. 12 No, 3, (2018), pp. 429.

- [62] Parker, D.B. Toward a New Framework for Information Security? In S. Bosworth, M.E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook*, 6th ed. (2015). (pp 3.1-3.23). Hoboken, NJ: John Wiley & Sons, Inc.
- [63] Gauthier, R., & Seker, R. Addressing Operator Privacy in Automatic Dependent Surveillance - Broadcast (ADS-B). In *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS)*, Waikoloa Village, HI, USA, (2018, January), pp. 52-61.
- [64] Strohmeier, M., Lenders, V., & Martinovic, I. On the Security of the Automatic Dependent Surveillance- Broadcast Protocol. *IEEE Communications Surveys & Tutorials*, Vol. 17 No. 2, (2015), pp. 1066-1087
- [65] Hopcraft, R., & Martin, K. M. Effective maritime cybersecurity regulation—the case for a cyber code. *Journal of the Indian Ocean Region*, Vol. 14 No. 3, (2018), pp. 354-366.
- [66] IUMI. IUMI Policy Agenda. (2020)
- [67] Ahvenjärvi, S., Czarnowski, I. and Mogensen, J. Addressing Cyber Security in Maritime Education and Training (CYMET). Final Report for the FY2018 IAMU, (2019).

Appendix

Appendix A: Example of vessel functions and related OT systems

| <i>Vessel function/service</i> | <i>OT system</i> |
|-----------------------------------|--|
| Water tight integrity | <ul style="list-style-type: none"> – Local and remote control, monitoring and alarm systems for: <ul style="list-style-type: none"> – water tight doors – shell doors – hatches |
| Power generation and distribution | <ul style="list-style-type: none"> – Local and remote control, monitoring and alarm systems for: <ul style="list-style-type: none"> – engine, turbine, generator, battery and other power sources – auxiliary machinery – Power management system – Power source safety system – Electrical circuit protection system |
| Propulsion | <ul style="list-style-type: none"> – Local and remote control, monitoring and alarm system for: <ul style="list-style-type: none"> – propulsion system (driver, shaft, gear, propeller, etc) – propulsion auxiliary machinery – Propulsion safety system |
| Steering | <ul style="list-style-type: none"> – Local and remote control, monitoring and alarm systems for: <ul style="list-style-type: none"> – steering (rudder, thruster, waterjet, etc.) – steering auxiliaries |
| Navigation | <ul style="list-style-type: none"> – Radar – Electronic chart display and information system (ECDIS) – Heading/gyro system – Autopilot – Automatic identification system (AIS) – Position reference system (GPS, etc.) – Voyage data recorder (VDR) – Bridge navigation watch alarm system (BNWAS) – CCTV – Navigation light system – Weather routing assistance system |
| Communication | <ul style="list-style-type: none"> – External communication system (GMDSS, satellite, radio etc.) – Internal communication system (PA, GA, telephone, radio etc.) |
| Drainage and bilge pumping | <ul style="list-style-type: none"> – Local and remote control, monitoring and alarm systems for bilge pumps, valve, sensors – Water ingress monitoring and alarm system |

| <i>Vessel function/service</i> | <i>OT system</i> |
|--------------------------------|---|
| Ballasting | <ul style="list-style-type: none"> – Local and remote control, monitoring and alarm systems for ballast pumps, valve, sensors – Load calculation system |
| Anchoring | <ul style="list-style-type: none"> – Anchor and winch control and monitoring system – Position mooring control system |
| Cargo operation | <ul style="list-style-type: none"> – Local and remote control, monitoring and alarm systems for cargo pumps, valve – Cargo level, pressure and temperature monitoring and alarm system – Cargo tank and other cargo-related safety systems – Inert gas control and monitoring system – Loading and offloading control and monitoring system – Crane control and monitoring system – Cargo conditioning, temperature, ventilation system |
| Fire and gas | <ul style="list-style-type: none"> – Fire detection system – Gas detection system (gas fuel) – Fire door control and monitoring system – Fire pump control and monitoring – Fire extinguishing systems |
| Ignition source control | <ul style="list-style-type: none"> – Gas detection system – Emergency shutdown system |
| Accommodation and passenger | <ul style="list-style-type: none"> – Ventilation and climate control system – Emergency safety/response system – Flooding detection system |
| Dynamic positioning | <ul style="list-style-type: none"> – Local and remote control, monitoring and alarm system for: <ul style="list-style-type: none"> – DP-thrusters and other driven units for positioning – auxiliary machinery – DP control system – Independent joystick system – DP sensors and reference systems |
| Drilling | <ul style="list-style-type: none"> – Hoisting control and monitoring system – Rotation control and monitoring system – Vertical pipe handling control and monitoring system – Horizontal pipe handling control and monitoring system – Well control and monitoring system – Mud and shaker control and monitoring system – Well intervention control and monitoring system – Manage pressure drilling control and monitoring system – Heave compensation control and monitoring system |

| <i>Vessel function/service</i> | <i>OT system</i> |
|--------------------------------|--|
| Oil and gas production | <ul style="list-style-type: none"> – Process control and monitoring system – Production safety system – Production skid local control and monitoring system – Production skid safety system – Subsea control and monitoring system – High integrity pressure protection system (HIPPS) |
| Other | <ul style="list-style-type: none"> – Auxiliary boiler control and monitoring system – Auxiliary safety system – Incinerator control and monitoring system – Main alarm system – Integrated control, monitoring, alarm and safety system – CCTV – Jacking control and monitoring system – Pollution prevention system |

Source: DNV GL [59]

Appendix B: Example of different consequences in maritime cybersecurity

| | <i>Consequence</i> | | |
|---|--|--|---|
| | <i>Low</i> | <i>Medium</i> | <i>High</i> |
| Violations of laws, regulations, or contracts | Violations of regulations and laws with minor consequences. Minor breaches of contract which result in at most minor contractual penalties. | Violations of regulations and laws with substantial consequences. Major breaches of contract with high contractual penalties. | Fundamental violations of regulations and laws. Breaches of contract with ruinous damage liabilities. |
| Impairment of the right to informational self-determination | Processing of personal data that could adversely affect the social standing or financial wellbeing of those concerned. | Processing of personal data that could have a seriously adverse effect on the social standing or financial wellbeing of those concerned. | Processing of personal data that could result in the injury or death of the persons concerned or that could endanger the personal freedom of the persons concerned. |
| Physical injury | Does not appear possible. | Physical injury to an individual cannot be absolutely ruled out. | Serious injury to an individual is possible. There is a danger to life and limb. |
| Impaired ability to perform tasks | Impairment was assessed to be tolerable for vessel. No risk of external impact (e.g. collision, grounding). | Impairment of the ability to perform some tasks at hand was assessed as intolerable for vessel. | Impairment of the ability to perform tasks was assessed as intolerable for vessel. |
| Negative internal or external effects | Only minimal impairment or only internal impairment of the reputation/trustworthiness of the organisation is expected. | Considerable impairment of the reputation/trustworthiness can be expected. | A nation-wide or world-wide loss of reputation/trustworthiness is conceivable, possibly even endangering the existence of the organisation. |
| Financial consequences | The financial loss is acceptable to the organisation. | The financial loss is considerable, but does not threaten the existence of the organisation. | The financial loss threatens the existence of the organisation. |

Source: DVN GL [59]

Appendix C: First-run questionnaire



Dear Participant,

We are research staffs 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 (attached) 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 are 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 message (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 is?

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 participant.

Appendix D: Second-run questionnaire



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 (Yera.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 to 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 | | | | | | | | | | | | | | | |
|--|----------------|---|---|-----------------|----|---|-----------------|----|----|----|----|---|---|---|----|
| | Likelihood (%) | | | Consequence (%) | | | Probability (%) | | | | | | | | |
| | VL | L | A | H | VH | N | MA | MO | CR | CA | HU | U | A | L | HL |
| 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.) | | | | | | | | | | | | | | | |
| Malware | | | | | | | | | | | | | | | |
| Accessing links from suspicious emails | | | | | | | | | | | | | | | |
| Downloading attached files from unknown emails | | | | | | | | | | | | | | | |
| Connecting USB or removable media to a computer without virus check | | | | | | | | | | | | | | | |
| Man-in-the-middle-attack | | | | | | | | | | | | | | | |
| 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 | | | | | | | | | | | | | | | |
| Accessing suspicious websites | | | | | | | | | | | | | | | |
| Connecting your infected USB or removable media to connect computers/navigation systems | | | | | | | | | | | | | | | |
| 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 login account system | | | | | | | | | | | | | | | |

| | Likelihood (%) | | | Consequence (%) | | | Probability (%) | | | | | | |
|--|----------------|---|---|-----------------|----|----|-----------------|----|----|---|---|---|----|
| | VL | L | A | N | MA | MO | CR | CA | HU | U | A | L | HL |
| | Likelihood (%) | | | Consequence (%) | | | Probability (%) | | | | | | |
| Providing personal information to a fake website (e.g. government website, etc.) | | | | | | | | | | | | | |
| Distributed Denial of Service (DDoS/DoS) | | | | | | | | | | | | | |
| DDoS attacks company's server system | | | | | | | | | | | | | |
| 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 | | | | | | | | | | | | | |
| Using outdated IT system | | | | | | | | | | | | | |
| Using outdated version firewall and antivirus 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
 - Port company
 - University
 - IMO
 - Other: _____

The questionnaire ends here. Thank you for your participant.

Appendix E: Deliverable 3 (Conference paper)

Cybersecurity in the maritime industry: a literature review

Changki Park^a, Wenming Shi^b, Wei Zhang^b, Christos Kontovas^a, Chia-Hsun Chang^{a*}

^a Liverpool John Moores University, 3 Byrom Street, Liverpool, L3 3AF, UK

^b Australian Maritime College, Maritime Way, Newham, Tasmania, 7248, Australian

*Corresponding author. E-mail: c.chang@ljmu.ac.uk

Keywords: cybersecurity, risk management, maritime industry

ABSTRACT

Cybersecurity has become an important issue in the maritime industry due to many reported cyberattack incidents that caused a lot of economy loss, personal or company information breach, and so on. However, there is limited research for maritime cybersecurity in the existing literature. This research aims to identify threats influencing cybersecurity in maritime operations and their control options through a state-of-the-art literature survey. A list of cyberattack incidents in various industries are presented. By restricting our attention to the maritime industry, this research identifies three maritime cyber threats, including the lack of training and experts, the use of outdated system, the risk of being hacker's target. To deal with the identified threats, a number of mitigation strategies are also proposed in this study, including developing cyber security process, providing cybersecurity training course, updating and upgrading programme regularly, and fostering cybersecurity climate.

1. Background

Around 80% of international trade is transported by sea [1]. At the same time, increased communication in international trade causes higher concerns on cyber-attacks as an emerging issue to maritime operations [2]. For example, Maersk, the largest container shipping company in the world, suffered a cyber-attack in 2017, which led to a loss of \$200-300 million [3]. The COSCO terminal in Port of Long Beach was cyberattacked in 2018 [4]. These cyber-attacks emphasize the importance of cybersecurity in the maritime industry as they caused not only economy loss, but also personal or company information breach, companies reputation harm, etc.

Cyber-attack incidents have resulted in unquantifiable losses of monetary assets, intellectual property, and customer confidence [5]. However, to the best of authors' knowledge, there is limited research for maritime cybersecurity in the existing literature. In the aspect of maritime cyber risk, it has been defined as 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 [6].

In order to deal with hazards in the maritime industry, risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the maritime industry [6]. Compared to other industries such as military, financing, airlines, cybersecurity related studies in the maritime industry is sitting at the backseat (e.g. ten to twenty years behind other computer-based industries [7]). In light of the above evidence, the authors have found that the cybersecurity in the maritime industry needs to be addressed in urgency. This research thus aims to identify threats

influencing cybersecurity in maritime operations and their control options through a state-of-the-art literature survey.

The rest of this paper is structured as follows. Section 2 reviews the definitions of cybersecurity and revisits cyberattack incidents in various industries. Section 3 identifies the cyber threats within the maritime industry. Section 4 proposes the potential control options. Discussion and conclusion are drawn in Section 5.

2. Literature review

2.1. The definition of cybersecurity

It has been used in a wide range of academic disciplines including computer science, engineering, political studies, psychology, security studies, management, education, and sociology [8]. Cybersecurity is commonly defined as “the protection of cyberspace as well as individuals and organizations that function within cyberspace and their assets in that space” [9]. [8] also re-defined cybersecurity as “the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure de facto property rights”.

2.2. Cyberattack incidents

The top 5 industries at greater risk of cyber-attack are government, financial services, manufacturing, education and law [10]. For instance, Department of Justice in the U.S was hacked in 2016, and it took a week for the organization to recover the system [11]. Equifax, an American credit company, had suffered a cyber-attack in 2017 and caused 143 million customers’ personal data were hacked, as well as 200,000 credit card numbers [12]. Marriott hotels had suffered cyberattack in 2018 and 500 million customers’ personal data were hacked [13].

2.3. Maritime cyberattack incidents

Comparing to the past, more and more maritime cyberattacks are reported in this decade due to the development of ICT and largely rely on such technology in the maritime industry. Table 1 lists the reported maritime cyberattack incidents from 2001 to 2018.

Table 1 Maritime cybersecurity incidents

| Year | Organization | Details |
|-----------|-------------------------------|--|
| 2011 | IRISL | An Iranian shipping line, IRISL, were cyberattacked in 2011 and lost all data related to rates, loading, cargo number, date and place. [14] |
| 2011-2012 | Port of Antwerp | Drug traffickers hired hackers to breach IT system of Port of Antwerp. Hackers accessed secure data giving them the location and security details of containers which contained heroin and cocaine. [15] |
| 2012 | Australian Border Force | This incident allowed criminals to check whether their shipping containers were regarded as suspicious by the Customs authorities. [16] |
| 2012-2014 | Danish Maritime Authority | Danish Maritime Authority was subjected to a cyberattack from 2012 but been discovered until 2014. The attack was introduced by a PDF document infected with a virus, and the virus was propagated from the Danish Maritime Authority to other government institutions. [17] |
| 2013 | Mobile Offshore Drilling Unit | A group of hackers remotely attacked a floating oil rig off the Gulf of Mexico and gained control of its stabilization systems and programmed the platform to tilt dangerously to one side. The platform had to be shut down for 19 days. [18] |
| 2016 | Korean vessels | South Korea reported that 280 vessels suffered problems with their navigational systems. The GPS signal was jammed by hackers; consequently, some of the GPS signals died and others received false information. [19] |

| | | |
|------|--------------------------------------|---|
| 2017 | Maersk | Maersk, the largest container shipping company in the world, was cyberattacked by a ransomware (NotPetya) in 2017, which shut downed Maersk's network system. It took almost three weeks to recover and caused a \$200-300 million financial loss. [3] |
| 2018 | COSCO terminal at Port of Long Beach | COSCO terminal at the port of Long Beach has been attacked by ransomware in July 2018 and took 5 days to recover. However, they did not suffer serious financial loss, as they took a lesson from Maersk incident in 2017 and separated their network in different servers. [20] |
| 2018 | Port of Barcelona | Hackers attacked several servers in the port's security infrastructure, without interrupting the maritime and land operations. [21] |
| 2018 | San Diego Port | The attack had not stopped vessels or boat using the port, or put members of the public in danger. The main impact would be on the issuing of park permits, public records requests and general business services. The Port said some of the disruption was because of staff shutting down computers that were in danger of being compromised as the ransomware started to spread. [22] |

Based on the above cyber-attacks reports, it can be found that the number of cyber-attack incidents in the maritime industry are increasing in this decade. The impacts of maritime cyberattack include economy loss, personal or company information breach, company's reputation harm, etc. Therefore, maritime cybersecurity is becoming an important issue that needs to be emphasized more than before.

3. Threats identification to maritime cybersecurity

This section identified several threats that impact on cybersecurity in the maritime industry from the existing literature, including the lack of training and expert, the use of outdated IT system, the risk of being hackers' target, and fake website and phishing email.

3.1. Lack of training and expert for cybersecurity

Human error has been previously identified as the most significant factor that causes around 80-90% of shipping accidents directly and indirectly [23], [24]. Human can be tired to make some mistakes that cause cyberattack incidents [25]. Cyberattacks might also come from unintentional actions via individuals with little or no cybersecurity training and awareness [26]. This allows malware to deliver through individual's activities. For example, computers are infected by accidentally open unknown e-mail and access false website with virus.

3.2. Use of the outdated IT system

[27] and [28] analysed vulnerability of cybersecurity in the maritime industry and found a major problem as the over reliance on outdated technology and security practices. For instance, maritime employees still believe that firewalls and antivirus software are sufficient to deal with cyberattacks. However, hackers can attack through viruses and other assorted malware and it is difficult for traditional antivirus software to deal with such advanced cyberattacks [27]. On the other hand, as large ships are expensive and take a long time to build, many ships were built before cybersecurity as a major concern. Thus, some vessels are still operating through outdated software systems that might cause cyberattack [28].

3.3. Risk of being hackers' target

Hacktivism is the most common threat for cybersecurity in the maritime industry [6]. Hacktivism has two types of actions: targeted and untargeted [26], [29], [30]. Targeted attacks refer to a company or a ship's systems and data are the intended target, hackers usually use tools and techniques specifically

created for a company or ship; whereas untargeted attacks are likely to use tools and techniques available on the internet, which can be used to locate, discover and exploit widespread vulnerabilities that may also exist in a company and on-board a ship [29].

[31] suggested that cyberattack with purpose would be practiced by three categories: hacktivism or activist group, terrorist group, and criminals. For hacktivism or activist group, they are made up of ideologically motivated people, for whom the main action is an online protest aimed at accessing the system and stealing sensitive information and data for malicious purposes. For terrorism, they can use electronic and computerized media as a new modus operandi to carry out their terrorist acts against other groups, nations, and companies, gaining access and interrupting the operating system, for ideological, religious or political interests or purposes. For criminals, individuals or criminal organizations use cyber-attacks against interconnected systems and networks, with the intention to carry out criminal activities, mainly focused on fraudulent operations, extortions or theft of intellectual property. It is also recognized that these criminals, when they obtain access to the different systems, can control operating systems to facilitate the trafficking of drugs, arms and contraband money to obtain economic benefits or to sell valuable information to another.

3.4. Fake website and phishing email

Sea crew using private devices (e.g. smart phone, tablet, personnel USB device, etc.) could cause cyberattacks through accessing fake websites and phishing emails, and further installing malicious virus into vessel system [32]. Malware is one of the well-known malicious software, which assesses or damages the victim's devices without the knowledge of the victim, and spread by opening infected email attachments or access fake website with malicious malware program such as Trojan horses, worms, exploits and backdoors [33]. Cyber incident of Petya and Notpetya have spread over the world recently. The idea of ransomware attacks is, encrypting and locking the files on a computer until the ransom is paid. These attacks usually enter the system by using Trojans, which has malicious programs that run a payload that encrypts and locks the files. The basic goal of this type of attack is getting money, so hackers usually unlock the files when they receive the money [34].

4. Risk control options for cyberattacks

4.1. Develop cybersecurity process

[6] and [29] recommended the functional elements that support effective cybersecurity process: identifying, protecting, detecting, responding, and recovering. In fact, there were some changes of cybersecurity process after huge cyber incident such as Maersk in 2017. COSCO has learnt the importance of cybersecurity process, and divided data in several servers. Therefore, when they suffered the cyberattack in 2018, they cut down the connection of the infected server and operated through other non-infected servers. In addition, their quick response and notification to customer was the reason to minimize risk of cyberattack [35].

4.2. Education and training for cybersecurity

In order to deal with the threat of lack of training and expert for cybersecurity, training sea crews and staffs may be an effective method to enhance maritime cybersecurity. [28] suggested that ship crews can be educated to deal with cyberattack by protection of password and access keys. Companies need to train their staffs and sea crews how to use digital equipment in a correct way, which can not only reduce the damage to the equipment, but also protect from cyberattacks. An event tree or standard operation process should be established to guide the staffs and sea crews to avoid or deal with cyberattacks. Companies can also follow the suggestion related to cybersecurity training from IMO

STCW (International Maritime Organization Standards of Training, Certification, and Watchkeeping) code and ISM (International Safety Management) code.

4.3. Upgrade and update system

In order to deal with the threat of use of the outdated IT system, it is necessary to keep update vaccine software and using updated program to mitigate cyber risk [36]. Through the development of advanced technology, many virus and malicious program are also created simultaneously. The maritime industry need to update or even upgrade IT system for not only keep their competitiveness, but also deal with the threat from cyberattacks.

4.4. Cybersecurity climate

Cybersecurity climate is a control option for cyber threat. This concept is adapted from safety climate, which is defined as the coherent set of perceptions and expectations that employees have regarding safety in their organization [37]. Safety climate can be used to proactively assess an organization's effectiveness in identifying and remediating work-related hazards, thereby reducing or preventing work-related ill health and injury [38]. Based on the above safety climate related literature, we develop cybersecurity climate as the environment of company to enhance awareness cyber risk and to prevent for cyber accident.

To foster cybersecurity climate in a company, several activities are adopted from safety climate, such as cybersecurity attitudes of management, cybersecurity education and training program, cybersecurity regulation and the status of security personnel, etc.

5. Conclusion

It has been growing relying many electronic and automated devices in maritime industry, cybersecurity issue has been increasing in this decade. Maritime industry is nationally and globally significant; the importance will be increased. Therefore, we focused on identifying cyber threats and developing risk control option in the maritime industry. In this study, four cyber threats have been identified, including lack of training and expert, use of the outdated IT system, Hacktivism, and fake site and phishing email. Four risk control options are also proposed, including developing cybersecurity process, education and training, upgrade and update system, and change cybersecurity climate.

For the further research, a set of interview will be conducted to validate the identified threats and risk control options and explore more if they are not identified from the literature review. Based on the results of interview, another questionnaire will be sent out to collect the likelihood, consequence, and probability of failure detection of each threat. Failure Modes and Effects Analysis (FMEA) with Fuzzy Rules Bayesian Network (FRBN) and Evidential Reasoning (ER) are used to evaluate the importance of the threats in maritime cybersecurity. Risk matrix will also be conducted to present in a simple and common way of the results to the maritime industry.

Acknowledgement

This project is funded by the International Association of Maritime Universities Young Academic Staff in FY2019.

6. REFERENCES

- [1] UNCTAD, *Review of Maritime Transport*, 2016, Available at: http://unctad.org/en/PublicationsLibrary/rmt2016_en.pdf
- [2] Svilicic, B., Kamahara, J., Rooks, M., & Yano, Y. (2019). Maritime Cyber Risk Management: An Experimental Ship Assessment. *The Journal of Navigation*, 72(5), 1108-1120.
- [3] Novet, J., Shipping company Maersk says June cyberattack could cost it up to \$300 million, 2017, Available at: <https://www.cnn.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html>
- [4] World Maritime News, COSCO Shipping Lines Falls Victim to Cyber Attack, 2018, Available at: <https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/>
- [5] Julisch, K., Understanding and overcoming cyber security anti-patterns, *Computer Networks*, 2013, 57 (1), 2206-2211.
- [6] IMO, guidelines on maritime cyber risk management, 2017 MSC-FAL.1/Circ.3REFERENCES.
- [7] Caponi, S., and Belmont, K. Maritime cybersecurity: A growing threat goes unanswered, *Intellectual Property and Technology Law Journal*, 2015, 27 (1), 16-18.
- [8] Craigen, D., Diakun-Thibault, N., & Purse, R. Defining cybersecurity, *Technology Innovation Management Review*, 2014, 4(10), pp.13-21
- [9] Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., and Kusev, P. Risk perceptions of cyber-security and precautionary behavior, *Computers in Human Behavior*, 2017, 75 (1), 547-559.
- [10] Bendovschi, A., Cyber-attacks—trends, patterns and security countermeasures, *Procedia Economics and Finance*, 2015, 28, pp. 24-31.
- [11] Department of Justice in the U.S cyberattack, 2016, Available at: <https://edition.cnn.com/2016/02/08/politics/hackers-fbi-employee-info/index.html>
- [12] Equifax, 2017, Available at: <https://www.bbc.co.uk/news/business-41575188>
- [13] Marriott hotels cyberattack, 2018, Available at: <https://www.bbc.co.uk/news/technology-46401890>
- [14] IRISL, 2015, Available at: https://www.joc.com/maritime-news/container-lines/carriers-threatened-cyber-attacks-experts-warn_20150303.html
- [15] Antwerp Bateman, T., Police warning after drug traffickers' cyber-attack, BBC News, 2013. Available at: <http://www.bbc.com/news/world-europe-24539417>
- [16] PORTSTRATEGY, 2017, Available at: <https://www.portstrategy.com/news101/port-operations/planning-and-design/cyber-security-feature>
- [17] Linton Art, Port Authority Role in Cyber-Security, Linked in, 2016, Available at: <https://www.linkedin.com/pulse/port-authority-role-cybersecurity-art-linton>
- [18] MODU, 2013, Available at: <https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities>
- [19] Saul, J., Cyber Threats prompt return of radio for ship navigation, Reuters, 2017, Available at: <https://www.reuters.com/article/us-shipping-gpscyber-idUSKBN1AN0H>
- [20] COSCO World Maritime News, COSOCO shipping lines falls victim of cyberattack, 2018, Available at: <https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/>
- [21] Information Security Newspaper, Hacking attack in port of Barcelona, 2018, Available at: <https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/>
- [22] BBC New, San Diego port hit by ransomware attack, 2018, Available at: <https://www.bbc.co.uk/news/technology-45677511>

- [23] Schröder-Hinrichs, J. U., ‘Human and Organizational Factors in the Maritime World – are We Keeping up to Speed?’, *WMU Journal of Maritime Affairs*, 2010, 9 (1), pp.1–3.
- [24] Heij, C. and Knapp, S., ‘Predictive Power of Inspection Outcomes for Future Shipping Accidents – An Empirical Appraisal with Special Attention for Human Factor Aspects’, *Maritime Policy and Management*, 2018, 45 (5), pp.604-621.
- [25] Cole, Connected Ships and Cybersecurity Frank J Coles, Transas CEO Shipping Insight Fleet Optimization Conference, 2017.
- [26] North P&I club, Cyber risk in shipping, North of England P&I group, 2017
- [27] Sen, R., Chapter 9. Cyber and information threats to seaports and ships. McNicholas, MA, *Maritime Security*, 2016, 2, pp. 281- 302
- [28] Jones, K. D., Tam, K., & Papadaki, M., Threats and impacts in maritime cyber security, 2016.
- [29] BIMCO, The Guidelines on Cyber Security Onboard Ships (Version 3), 2018.
- [30] Ahokas Jenna, The Finnish maritime sector and cybersecurity, *PUBLICATIONS OF THE HAZARD PROJECT*, 2019, University of Turku.
- [31] IET, Code of Practice, *Cyber security for Ports and Port System*, Available at: <https://cybersail.org/wp-content/uploads/2017/02/IETCyber-Security-Code-of-Practice-for-Ports-Port-Systems.pdf>
- [32] Japan P&I Club, Cyber risk and Cyber security countermeasures, 2018, Available at: <https://www.piclub.or.jp/wp-content/uploads/2018/05/Loss-Prevention-Bulletin-Vol.42-Full.pdf>
- [33] Teoh, C.S. and Mahmood, A.K., Cybersecurity Workforce Development for Digital Economy. *The Educational Review*, 2018, USA, 2(1), pp.136-146.
- [34] Fayi, S.Y.A., What Petya/NotPetya ransomware is and what its remediations are, *In Information Technology-New Generations*, pp. 93-100, Springer, Cham.
- [35] COSCO JCO.com, Cosco’s pre-cyberattack efforts protected network, 2018, Available at: https://www.joc.com/maritime-news/container-lines/cosco/cosco%E2%80%99s-pre-cyber-attack-efforts-protected-network_20180730.html
- [36] Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). The future of maritime cyber security, 2015, Lancaster University.
- [37] Zohar, D., Safety climate in industrial organizations: theoretical and applied implications. *Journal of Applied Psychology*, 1980, 65, pp. 96-102.
- [38] Schwatka, N. V., Hecker, S., & Goldenhar, L. M., Defining and measuring safety climate: a review of the construction industry literature. *Annals of occupational hygiene*, 2016, 60(5), pp. 537-550.

Appendix F: Deliverable 4 (Presentation in AGA20)






Cybersecurity in the maritime industry

Chia-Hsun Chang (LJMU)
 Wei Zhang (AMC)
 Wenming Shi (AMC)
 Changki Park (LJMU)

1

dream plan achieve




Introduction

- Maersk lost \$200-300 million in 2017
- COSCO terminal in Long Beach in 2018
- Losses of monetary asset, intellectual property, and customer confidence (Julisch, 2013)
- Compared to other industries, cybersecurity in the maritime industry is sitting at the backseat
- This project aims to address cybersecurity in the maritime industry through three objectives:
 - Obj1: Identify threats influencing cybersecurity in maritime operations
 - Obj2: Evaluate the importance of the identified threats
 - Obj3: Provide solutions to controlling the identified threats

2

dream plan achieve




Description of work packages

- WP1: Initial team meeting
- WP2: Identify maritime cyber threats
- WP3: Identify the importance of the threats
- WP4: Evaluate the importance of the threats
- WP5: Provide solutions to controlling the identified threats

3

dream plan achieve




Definition of cybersecurity

- “the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure de facto property rights” (Craig, Diakun-Thibault, and Purse, 2014)
- “the protection of cyberspace as well as individuals and organizations that function within cyberspace and their assets in that space” (Schaik et al., 2017)

4

dream plan achieve



Cyberattack incidents

- 2016, Department of Justice in the U.S: it took a week to recover the system (Mallonee, 2016)
- 2017, Equifax: 143 million customers' personal data were hacked, as well as 200,000 credit card numbers (BBC, 2017)
- 2018, Marriott hotels: 500 million customers' personal data were hacked (BBC, 2018)

5

dream plan achieve



Maritime cyberattack incidents

- More than 10 maritime cyberattacks incidents from 2011
- 2016, 280 Korean vessels: The GPS signal was jammed by North Korean
- 2017, Maersk: NotPetya, \$200-300 million financial loss in 2 weeks
- 2018, COSCO terminal at Port of Long Beach: system shutdown for 5 days
- 2018, Port of Barcelona: no impact on port operations, but port's security infrastructure
- 2018, Port of San Diego: no impact on port operations, but to park permits, public records requests and general business services
- 2018, Australian defence shipbuilder Austal: unclassified ship designs
- 2018, Ukrainian ships: cyberattacked by Russia
- 2018, U.S. Navy: Chinese hackers had repeatedly stolen information from Navy contractors including ship maintenance data and missile plan.
- 2019, U.S. Coast Guard

6

dream plan achieve

LIVERPOOL JOHN MOORES UNIVERSITY

Threats identification to maritime cybersecurity

- Human error
- Using outdated IT system
- Phishing
- Malware
- Ransomware
- Theft of credential
- Man in the middle attack
- DDoS

7 dream plan achieve

LIVERPOOL JOHN MOORES UNIVERSITY

Interview to validate and explore threats

There are 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 message (e.g. bank, credit card company, insurance company, etc.) | |
| Other (please specify): | |
| Malware | |
| Downloading files (e.g. mp3, movie, games) from suspicious websites | |

8 dream plan achieve

LIVERPOOL JOHN MOORES UNIVERSITY

Questionnaire designing

Part 1: There are 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 | LN | N | MA | MO | CS | CA | HU | W | A | L | HL |
| Accessing links from impersonation emails (e.g. bank, credit card company, insurance company, etc.) | 40 | 50 | 10 | | 20 | 40 | 30 | 10 | | | | | | | 100 |
| Downloading attached files from impersonation emails (e.g. bank, credit card company, insurance company, etc.) | | | | | | | | | | | | | | | |
| Accessing links from impersonation text message (e.g. bank, credit card company, insurance company, etc.) | | | | | | | | | | | | | | | |
| Malware | | | | | | | | | | | | | | | |
| Malware | Likelihood (%) | | | | Consequence (%) | | | | Probability (%) | | | | | | |
| | VL | L | A | H | LN | N | MA | MO | CS | CA | HU | W | A | L | HL |
| Downloading files (e.g. mp3, movie, games) from suspicious websites | | | | | | | | | | | | | | | |
| Accessing links from suspicious emails | | | | | | | | | | | | | | | |

9 dream plan achieve

LIVERPOOL JOHN MOORES UNIVERSITY

Data analysis methods

- Failure Modes and Effects Analysis (FMEA)
 - RPN = likelihood × consequence × probability of undetected
- Rule-based Bayesian Network (RBN) and Evidential Reasoning (ER)

10 dream plan achieve

LIVERPOOL JOHN MOORES UNIVERSITY

RBN with a belief structure

| Rule | Parameters in the IF part | | | DoS in the THEN part | | | | |
|------|---------------------------|-------------------|--------------------|----------------------|------|------|------|------|
| | L | C | P | R1 | R2 | R3 | R4 | RS |
| 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 |

11 dream plan achieve

LIVERPOOL JOHN MOORES UNIVERSITY

Conditional probability table (CPT)

| L | L1 | | | | L5 | | | |
|----|----|------|------|------|------|------|------|----|
| | C1 | C5 | C1 | C5 | P1 | P5 | P1 | P5 |
| 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 |

12 dream plan achieve

LIVERPOOL JOHN MOORES UNIVERSITY

Data analysis methods

- 3D risk matrix
- T-test/ANOVA
 - UK vs Australia
 - Departments
 - Positions

13

dream plan achieve

LIVERPOOL JOHN MOORES UNIVERSITY

Risk control options (RCOs)

- Cybersecurity education and training:
 - IMO STCW (International Maritime Organization Standards of Training, Certification, and Watchkeeping) code and ISM (International Safety Management) code.
- Malware protection software installation
- Software update:
 - update or even upgrade IT system to keep competitiveness and deal with cyberattacks
- Password policy

14

dream plan achieve

LIVERPOOL JOHN MOORES UNIVERSITY

Risk control options (RCOs)

- Developing cybersecurity process
 - IMO, BIMCO, DNV-GL, ABS, etc. propose guideline and regulation
- Enhancing cybersecurity awareness

15

dream plan achieve

LIVERPOOL JOHN MOORES UNIVERSITY

Thank you

16

dream plan achieve



International Association of Maritime Universities

Meiwa Building 8F, 1-15-10 Toranomom, Minato-ku, Tokyo 105-0001, Japan

Tel : 81-3-6257-1812 E-mail : info@iamu-edu.org URL : <http://www.iamu-edu.org>

ISBN No. 978-4-907408-35-0