JOURNAL OF MARITIME RESEARCH

Vol XXIII. No. I (2026) pp 17–24

**ISSN: 1697-4840,** **www.jmr.unican.es**

# The Evaluation of Awareness of Cyber Security in Shipping Operations Among Malaysian Seafarers

Nor Hazlinda Nordin[1], Capt. Dr. Mohammad Ismail Russtam Suhrab[1,*]

*ARTICLE INFO*

***Article history:***
Received 31 Dec 2024;
in revised from 24 Jan 2024;
accepted 05 Apr 2025.

***Keywords:***
Maritime Cyber Security, Malaysian Seafarer Awareness, Shipping Operations Security, Maritime Cyber Attack.

*ABSTRACT*

The rapid development of the digitalization world has influenced maritime industries to upgrade their manually human-operated system to the technology of automatic and digital systems, increasing efficiency and exposing the sector to cyber threats. This research identifies key factors influencing cybersecurity in maritime security through expert interviews and assesses seafarers' awareness levels using surveys and thematic analysis. It shows that cyber security factors in shipping operations were based on two main factors: human error and the system in shipping operations. This study evaluates the cybersecurity awareness among Malaysian seafarers, focusing on their understanding of risks, preparedness for cyberattacks, and the effectiveness of existing initiatives to enhance cybersecurity awareness. Regression analysis is employed to evaluate data trends and relationships further. Despite ongoing initiatives by maritime organizations, such as cybersecurity guidelines and training courses, the rise in cyberattack cases calls into question the effectiveness of these measures. Findings reveal significant gaps in awareness, highlighting the need for improved training and organizational support. This research proposes actionable recommendations to enhance cybersecurity awareness, including tailored training programs, regular cybersecurity drills, and updates on emerging threats. By addressing these gaps, this research contributes to strengthening the resilience of Malaysian seafarers and the maritime industry against evolving cyber threats, ensuring safer and more secure shipping operations.



## 1. Introduction.

### *1.1. Research Background.*

The maritime industry is also not excluded from the Cybertechnologies era. The development of the digitalization world has influenced all industries to upgrade their manually human-operated system to the technology of automatic and digital systems.

The serious challenges of securing data from any cyberattack need to be considered. In 2017, IMO announced its encouragement to raise awareness and cybersecurity to ensure the ship's and crew's safety onboard. This research paper aims to evaluate cyber security awareness in shipping operations among Malaysian seafarers. As such, maritime organizations have organized initiatives to raise awareness among seafarers, such as establishing guidelines, courses, etc., but the effectiveness of those initiatives still needs to be evaluated. The scope of this research focuses on the level of awareness of seafarers on the cyberattack situation among Malaysian seafarers. The respondents of this research targeted active seafarers with Malaysian citizenship regardless of where they were working onboard. The respondents also included the marine operators who were involved in shipping operations. However, this research does not include the foreign seafarers who work on Malaysian ships.

### *1.2. Statement of the Problem.*

It is crucial to ensure the shipping operation and management data are secure. The vulnerable maritime systems, such as navigation systems, shipping systems, passengers' details,

[1]Faculty of Maritime Studies, Universiti Malaysia Terengganu, 20130, Kuala Nerus, Terengganu, Malaysia.
[*]Corresponding author: Capt. Dr. Mohammad Ismail Russtam. E-mail Address: m.ismail@umt.edu.my.

cargo details, and much more, are secured in private and have limited access by the shipping company only. However, using networking systems to save and share data can lead to cyber risk. Maritime cyber risk refers to the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety, or security failures due to information or systems being corrupted, lost, or compromised (IMO, 2021).

The International Maritime Organization (IMO) published The Guidelines on Maritime Cyber Risk Management as a recommendation to manage maritime cyber risk, especially in managing and safeguarding shipping from current and emerging cyber threats and vulnerabilities. However, the increase in successful cyberattacks has put all shipping operations at risk. As the operators and seafarers onboard are expected to be able to handle the problem to avoid the cases, therefore IMO (2017) announced the urgent need to raise awareness of cyber threats and vulnerabilities to support safe and secure shipping.

### *1.3. Research Questions.*

- What are the factors of cyber security in the maritime industry?
- What is the level of awareness of seafarers? In the cyberattack situation.
- How to increase the awareness of Malaysian seafarers on cyber security in Shipping operation?

### *1.4. Objectives of the Research.*

- To identify the factor of cyber security in maritime security.
- To evaluate the level of awareness of seafarers on the cyberattack situation.
- To propose the recommendation to raise. The level of awareness of seafarers on cyber security in shipping operations.

### *1.5. Justifications for Research.*

As the demand for shipping operations increases, more data must be secured in the shipping industry. In 2017, IMO announced its encouragement to raise awareness and cybersecurity to ensure the ship's and crew's safety onboard. According to research by Det Norske Veritas (DNV, 2023), the organization stated that the risk of maritime cyber threat had escalated, and their organizations have made it a significantly higher priority to secure shipping operational technology. The shipping operational technology manages, monitors, controls, and automates physical assets, such as sensors, switches, safety and navigation systems, and vessels.

This research paper aims to evaluate cyber security awareness in shipping operations among Malaysian seafarers. As such, maritime organizations have organized initiatives to raise awareness among seafarers, such as establishing guidelines, courses, etc., but the effectiveness of those initiatives needs to be evaluated. The awareness of cyber security is very important to be developed at a large scale as if the technology in the maritime operation fails, the seafarers are expected to handle the problem and provide a solution to prevent the cyberattack from causing a lot of damage to vessels and loss of data privacy. It is, therefore, necessary to focus on the seafarers' awareness when preventing maritime cyberattacks.

Canepa et al. (2021) conclude that a lack of knowledge of security procedures and awareness is a common issue further exacerbated by the rapidly changing technological scenarios. As the level of awareness is still low among Malaysian seafarers, maritime organizations and shipping companies can take the initiative to enhance awareness to prepare seafarers for cyberattacking. The level of awareness shall be evaluated to measure the effectiveness of all the efforts made to raise awareness of the cyberattack situation. If the awareness is at an elevated level, the methods shall remain. However, if the level of awareness is still low, the method used shall be invented to create another method to raise awareness. Therefore, this research paper also aims to propose recommendations to increase or maintain awareness among seafarers in Malaysia.

## 2. Literature Review.

Mission Secure (2010) defines maritime "cybersecurity" as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies used to protect organizations, vessels & their cyber environment.

According to Rachel Hand (2022), "shipping operations" refer to the processes involved in transporting merchandise from one place to another. Shipping operations involve the seller sending goods to the buyer using a shipper to transport the goods.

According to the Malaysian Federal Legislation, Merchant Shipping Ordinance Act A1519 (2016), "seafarer" means any person employed or engaged in any capacity on board a ship to which this Ordinance applies.

However, seafarers do not include people not directly employed for the normal manning of the ship within the deck, engine, or catering department. Plus, the term seafarers does not apply to pilot, superintendent, surveyor, auditor, inspector, supernumerary, scientist, researcher, diver, specialist offshore technician, or any person whose work is not part of the routine business of the ship. A person who works on board the ship solely within a port or at a port facility as a repair and maintenance technician is not considered a seafarer. Based on data from the Malaysia Marine Department (2018), the total number of active Malaysian seafarers is 694,551, and non-active Malaysian seafarers are 469,360.

A few factors influence cyber security in shipping operations. Below are the factors that the previous researchers have simplified.

Table 1: The Factors that Influencing Cyber Security in Shipping Operation.

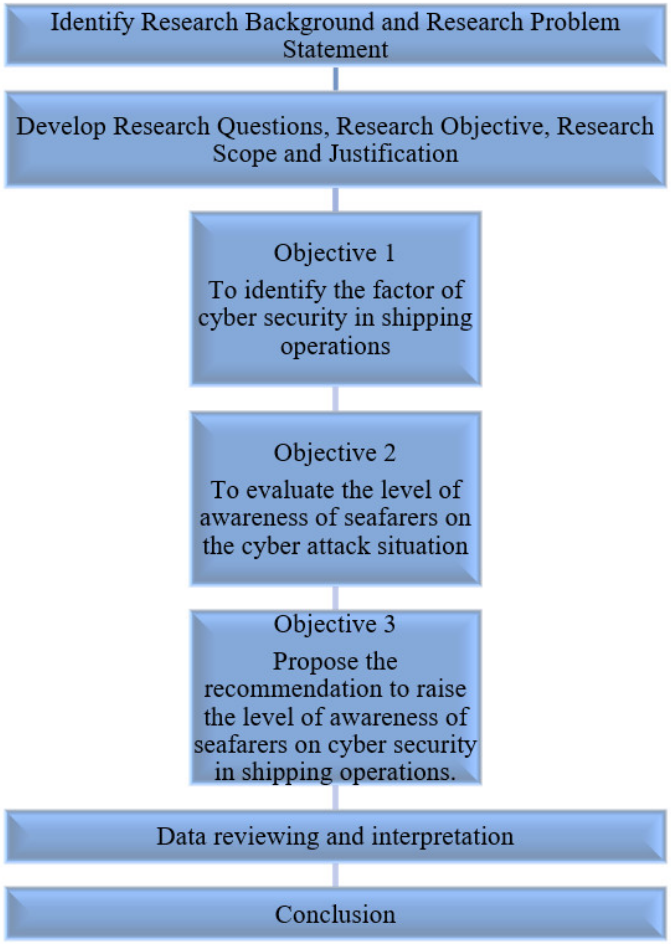
| Author | Year | Title | Factors that Influencing Cyber Security in Shipping Operations |
|---|---|---|---|
| Kanwal et al. | 2022 | Maritime cybersecurity: are onboard systems ready? | - Human error<br>- Employees are not trained to respond appropriately to cyber threats<br>- Outdated software systems also pose a tangible cybersecurity risk |
| Meland et. Al. | 2021 | A Retrospective Analysis of Maritime Cyber Security Incidents | - Increased connectivity and the converging of Information Technology (IT) and Operation Technology (OT) systems will expose maritime operations to new threats |
| Hareide et. Al. | 2018 | Enhancing Navigator Competence by Demonstrating Maritime Cyber Security | - Errors introduced in a critical system such as the ECDIS<br>- Incompetence employees |
| Afenyo and Caesar | 2023 | Maritime cybersecurity threats: Gaps and directions for future research | - Infection of critical port infrastructure with malware and ransomware.<br>- Inadequacies of the maritime cyber security literature and practice<br>- - Lack of proper human training and the lack of organizational framework |

Source: Authors.

## 3. Methodology.

### *3.1. Research Framework Design.*

Figure 1: Research Framework Design of the Research.




Source: Authors.

The research framework used for this research is the Exploratory Sequential Mixed Methodology. It is a practical roadmap that outlines the identification of the research background and problem statement, the development of the research questions and objectives, the data collection method, data analysis, data review and interpretation, and the conclusion of the research project. The research framework of this research is built up to provide step-by-step guidance for conducting the research study.

This research will start by identifying the research background and research problem statement. A literature review will be done to gain knowledge regarding the problem statement and the research problem statement.

The next step is to develop research questions and research objectives. This research focuses on the level of awareness regarding the cyberattack situation among Malaysian seafarers. The respondents of this research targeted active Malaysian seafarers. Then, the statement to justify this research.

The literature review will also give us some ideas on how to collect data. For the first objective, which is to identify the factors of cyber security in shipping operations, the analysis method used is Thematic Analysis, and the data collection method by the literature review & interview the experts to verify the factors of cyber security in shipping operations that are found in the literature review.

The data collection process for the second objective, to evaluate seafarers' awareness of cyberattack situations, will be conducted by interviewing experts in cyber security and shipping operations. The survey aims to achieve the first objective: identify cyber security factors in shipping operations. Then, data will be collected by questionnaires to the Malaysian seafarers. The questionnaires aim to reach 384 active Malaysian seafarers, selected randomly using the Krejcie and Morgan sampling method. The data will then be analyzed using the regression analysis method.

For the third objective, to propose a recommendation to raise seafarers' awareness of cyber security in shipping operations, the analysis method is Thematic Analysis, and the data collection methods are literature review and interview.

After all the data have been collected, it will be analyzed. Data analysis for this research will use thematic analysis and regression analysis. The thematic analysis will be used to analyze the data for the first and third objectives, and the regression analysis will be used to analyze the data for the second objective. Then, all data will be reviewed and interpreted in infographics such as graphs. Lastly, a conclusion will be made to conclude all the findings from the research.

### *3.2. Data Collection Strategy.*

The data collected from the Malaysian seafarers are primary, as they are first-hand and have not yet been processed. The type of data is quantitative data. Data for this research is collected using questionnaires that will be distributed online using Google Forms. The questionnaires will be distributed to Malaysian Seafarers through e-mail, WhatsApp's group, and all seafarers' groups on social media that can be reached.

### 3.3. Sampling Strategy.

The sampling method for this research is simple random sampling, as the respondents will be selected randomly among all Malaysian seafarers. The sampling population for this research only focuses on active Malaysian seafarers. According to the Malaysia Marine Department's database (2018), the total number of active Malaysian Seafarers is 694,551.

The Krejcie and Morgan (1960) sampling method determines this research's sampling size. Krejcie and Morgan's sampling size is commonly used to estimate the appropriate sample size for research studies. It is used when researchers cannot access the entire statistical population of interest and must make decisions based on a representative sample.

Referring to the Krejcie and Morgan table, the total sample size for 694,551 total population size is 384. This means that this research required 384 respondents who were active Malaysian seafarers.

### 3.4. Types of Analysis Methods Applied.

This research will analyze the data collected using the Thematic and Regression analyses.

The first methodology for this research is Thematic Analysis. The thematic analysis identifies and understands major themes and their relationships within qualitative data. It provides a high-level and wide-angle view. The data from interviewing the experts regarding the factor of cyber security in maritime security will be evaluated by Thematic Analysis.

The second methodology is Regression Analysis. Regression analysis is a set of statistical methods to estimate relationships between a dependent variable and one or more independent variables. Regression allows researchers to predict or explain the variation in one variable based on another variable. It can be utilized to assess the strength of the relationship between variables and to model the future relationship between them. The data from surveys from random active Malaysian seafarers will be interpreted in charts and graphs by using the equation below:

Formula of Regression Analysis:

$$Y = a + bX + e \quad (1)$$

Y = Dependent variable,
X = Independent variable,
a = Intercept,
b = Slope,
e = Residual (error).

## 4. Results and Discussions.

### 4.1. The Factors on Cyber Security in the Maritime Industry.

As the research was conducted, the data collected were analyzed and concluded according to the related research objectives. The first objective is to identify the factors of cyber security in maritime security. The data collective method for this objective is revising the literature review and expert interviews. The data will be analyzed using the Thematic Analysis method.

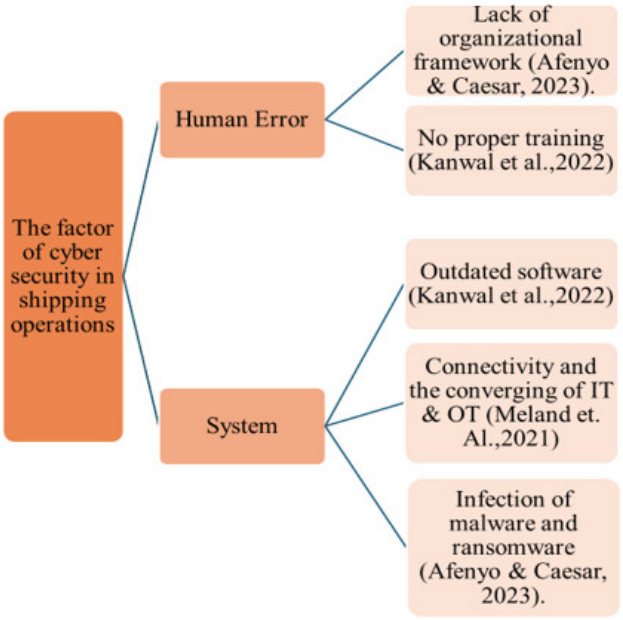
The outcomes of this research are the factors of cyber security in shipping operations as follows:

Table 2: Factors that Influencing Cyber Security in Shipping Operation.

| Factors that Influencing Cyber Security in Shipping Operations |
|---|
| Human error influences cyber security in shipping operations as employees are not trained to respond appropriately to cyber threats. (Kanwal et al.,2022) |
| Outdated software systems also pose a tangible cybersecurity risk (Kanwal et al.,2022) |
| Increased connectivity and the converging of Information Technology (IT) and Operation Technology (OT) systems will expose maritime operations to new threats (Meland et al.,2021) |
| Infection of critical port infrastructure with malware and ransomware and the maritime cyber security literature and practice inadequacies are cyber security factors (Afenyo & Caesar, 2023). |
| Lack of proper human training and organizational framework affect cyber security (Afenyo & Caesar, 2023). |

Source: Authors.

Figure 2: The Factor of Cyber Security in Shipping Operation.




Source: Authors.

The result of the first objective shows that cyber security factors in shipping operations were based on two main factors: human error and the system in shipping operations. According to the Maritime Transportation Research Board of the USA, human error in the maritime domain is "the commission or omission of acts by maritime personnel that cause or contribute to merchant marine casualties or near-casualties" (MTR, 2021).

Figure 2 illustrates two primary factors influencing cybersecurity in shipping operations. Human Error involves two key challenges. First, the lack of organizational framework (Afenyo & Caesar, 2023) arises when maritime organizations do not establish clear cybersecurity guidelines, leaving employees unsure of their responsibilities, which can lead to mistakes and breaches. Second, the lack of proper training (Kanwal et al., 2022) highlights the importance of educating seafarers and employees. Without adequate training, personnel may inadvertently introduce cyber risks, such as falling victim to phishing or failing to follow security protocols.

On the System side, several issues contribute to cybersecurity risks. Outdated software (Kanwal et al., 2022) can leave systems vulnerable to cyberattacks, as old software often contains unpatched security flaws. Additionally, the convergence of IT and OT (Meland et al., 2021) increases exposure to cyber threats, as integrating operational and information technology systems can create new vulnerabilities. Finally, the infection of malware and ransomware (Afenyo & Caesar, 2023) represents a significant risk, as malicious software can disrupt operations, steal data, or demand ransom payments.

Addressing these factors requires a comprehensive approach involving training, improved organizational frameworks, and system updates.

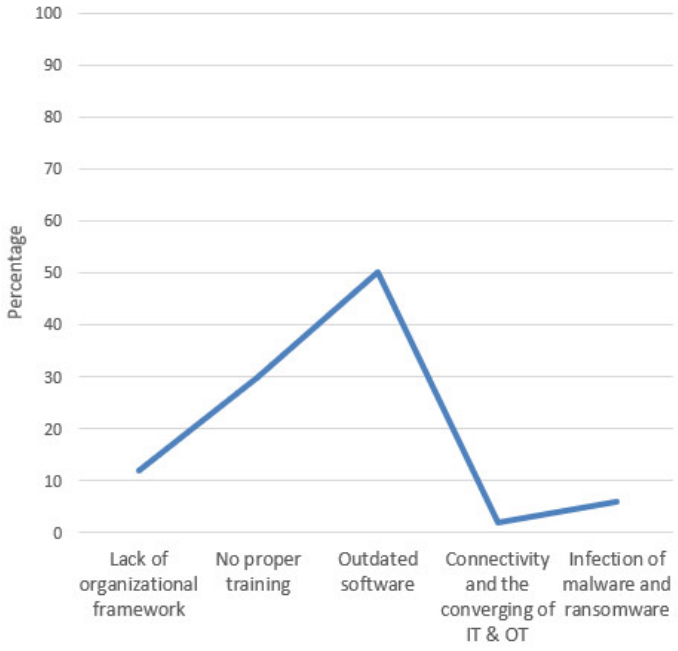
### 4.2. *The Level of Awareness of Seafarers on the Cyberattack Situation.*

The second result of the research is to evaluate seafarers' awareness of the low cyberattack situation in shipping operations. The early hypothesis is based on research from Canepa et al. (2021), as they conclude that the lack of awareness is due to the lack of knowledge of security procedures.

According to the Malaysia Marine Department database (2018), the total number of active Malaysian seafarers is 694,551. The sampling size of this research was determined by using the Krejcie and Morgan (1960) sampling method, which required 384 active Malaysian seafarers as respondents. However, due to restricted time, this research only managed to reach 100 respondents. Based on the survey of 100 Malaysian seafarers, below is the data that can be concluded on the level of awareness of seafarers on the cyberattack situation in shipping operations.

The graph illustrates varying levels of awareness regarding key cybersecurity challenges in maritime operations. It identifies five critical areas: lack of organizational framework, proper training, outdated software, connectivity, the convergence of IT (Information Technology) and OT (Operational Technology), and infection of malware and ransomware. IT (Information Technology) deals with systems that manage, process, and store data, such as networks, servers, software, and communication technologies. It focuses on the digital infrastructure for data management, cybersecurity, and communication. Examples are enterprise networks, e-mail systems, cloud computing, and database management. OT (Operational Technology) involves hardware and software systems that monitor, control, and operate physical processes, machinery, and industrial equipment. It focuses on the operational and automation aspects of manufacturing, energy, and maritime operations. Examples: SCADA (Supervisory Control and Data Acquisition), Industrial Control Systems (ICS), and ship engine monitoring systems.

Figure 3: The awareness of seafarers on the factor of cyberattack.




Source: Authors.

The graph starts with a lack of organizational framework, where awareness is notably low, around 10%. This suggests that many people are unaware of the importance of having a structured cybersecurity framework to protect maritime systems. Moving to no proper training, awareness increases steadily, reflecting a growing recognition of how inadequate or insufficient training exposes maritime operations to cyber threats.

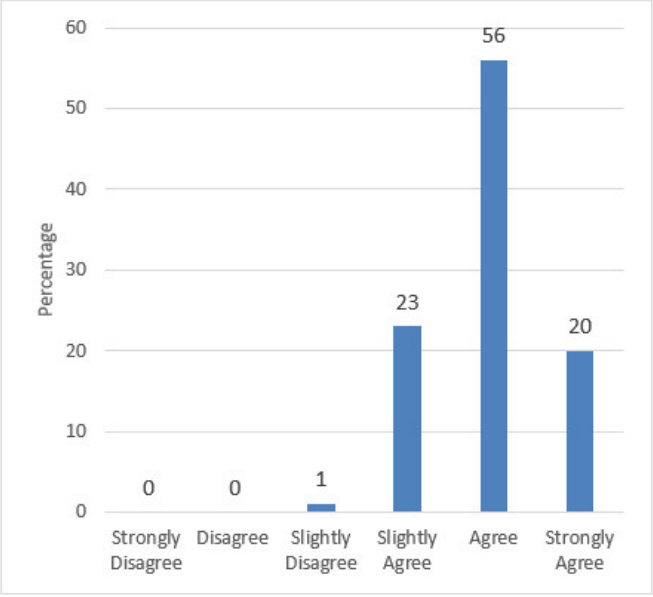
The peak in the graph is with outdated software, where awareness reaches approximately 50%. This indicates that outdated software is the most widely recognized challenge, likely due to its association with known vulnerabilities that hackers can exploit. However, awareness drops significantly when addressing connectivity and the convergence of IT and OT systems, falling close to zero. This sharp decline highlights a critical gap in understanding the risks associated with integrating operational and digital technologies, which are increasingly interconnected in modern maritime operations.

Finally, awareness of infection from malware and ransomware remains extremely low, showing only a slight increase. This is concerning, given the prevalence of malware and ransomware

attacks in maritime and other industries.

The graph reveals inconsistent awareness levels across different cybersecurity issues, with outdated software being the most recognized concern. However, the lack of awareness regarding connectivity risks and malware infections highlights significant gaps that must be addressed. Improving training, organizational frameworks, and educational efforts is essential to enhance cybersecurity awareness and preparedness in maritime operations.

Figure 4: Seafarers' awareness of the basic cyber security concepts, such as viruses, malware, and phishing.




Source: Authors.

The data reflects the level of awareness among seafarers regarding basic cybersecurity concepts such as viruses, malware, and phishing. The results indicate that most respondents possess a considerable degree of awareness. Most participants (**??**) "Agree" that they are familiar with these concepts, while 20 respondents "Strongly Agree," indicating an elevated level of confidence in their knowledge. Additionally, 23 respondents "Slightly Agree," suggesting moderate awareness. Only one individual "Slightly Disagrees," and none fall into the "Disagree" or "Strongly Disagree" categories. This highlights that awareness of fundamental cybersecurity issues is widespread among the surveyed group, with minimal indications of insufficient knowledge.

Cybersecurity protects digital systems, networks, devices, and data from unauthorized access, theft, damage, or malicious activities. It encompasses a range of technologies, processes, and practices designed to defend against cyber threats such as hacking, malware, phishing, and ransomware. The primary objectives of cybersecurity are to ensure confidentiality by safeguarding sensitive information, maintain integrity by preventing unauthorized alterations, and guarantee availability by ensuring systems and data remain accessible to authorized users. Covering various areas like network, application, cloud, and information security, cybersecurity is a constantly evolving field that requires continuous updates and vigilance to combat emerging threats.

A computer virus is malicious software designed to replicate and spread to other devices, often without the user's knowledge. It attaches itself to legitimate programs or files and executes harmful actions, such as corrupting or deleting data, slowing system performance, or causing complete system failures. Viruses typically spread through infected e-mail attachments, downloads, or removable storage devices. According to Kaspersky (2023), viruses are one of the most common types of malware and can severely disrupt personal and organizational systems if not properly mitigated. To protect against viruses, using updated antivirus software, avoiding suspicious files, and regularly updating operating systems and applications are critical steps.

Malware, short for "malicious software," refers to any software designed to harm, exploit, or disrupt devices, networks, or services. Common types of malware include viruses, worms, Trojans, ransomware, spyware, and adware. Malware can infiltrate systems through phishing e-mails, malicious websites, or infected files, with effects ranging from data theft to system hijacking and unauthorized surveillance. Symantec (2023) notes that malware attacks are becoming increasingly sophisticated, making it essential to use comprehensive cybersecurity measures like firewalls, reputable security software, automatic updates, and user education on safe online practices.

Phishing is a social engineering tactic where attackers trick individuals into disclosing sensitive information, such as passwords or financial data. It often involves fraudulent e-mails, messages, or websites disguised as legitimate sources, such as banks or trusted organizations. Phishing attacks exploit human trust and urgency, prompting users to act without verifying the authenticity of the communication. According to the Anti-Phishing Working Group (APWG, 2023), phishing attacks have significantly increased in recent years, targeting individuals and businesses. Combating phishing requires cautious behavior, verifying sender identities, avoiding clicking on suspicious links, and implementing multi-factor authentication for enhanced security.

This indicates that awareness of basic cybersecurity issues is widespread among the surveyed group, with minimal indications of insufficient knowledge. By understanding the threats posed by viruses, malware, and phishing, individuals and organizations can better prepare to protect their digital environments and data from these increasingly prevalent cyber risks.

### *4.3. Recommendation to Increase the Awareness of Malaysian Seafarers on Cyber Security in Shipping Operations.*

Lastly, the research outcome proposes a recommendation to raise seafarers' awareness of cyber security in shipping operations. Referring to previous research, below are the initiatives to raise seafarers' awareness of cyber security in shipping operations.

Figure 5: Recommendation to raise the level of awareness of seafarers on cyber security in shipping operations.


Source: Authors.

The result emphasizes the critical need to raise seafarers' awareness of cybersecurity in shipping operations by outlining key recommendations supported by research. Cybersecurity in maritime operations is a growing concern due to the increasing reliance on digital systems for communication, navigation, and logistics. As ships and ports adopt advanced technologies, they become more vulnerable to cyber threats like hacking, malware, and phishing attacks. Therefore, improving the cybersecurity awareness of seafarers and maritime personnel is essential to safeguard operations, protect assets, and ensure the safety of crew and cargo.

The first recommendation focuses on providing proper training for employees of maritime-related institutions. Zhang and Albert (2019) emphasize that employees must be trained to handle and respond to cybersecurity issues effectively. Training equips them with the necessary skills and knowledge to identify potential cyber threats, respond to breaches, and implement preventive measures. Proper training improves individual competence and contributes to building a culture of cybersecurity awareness within maritime organizations.

Secondly, the chart highlights the importance of providing sea crews with sufficient knowledge through regular and comprehensive training. According to Kanwal et al. (2022), consistent training helps mitigate the impact of cyberattacks by ensuring that sea crews are well-prepared to detect and respond to threats. Shipping operations rely heavily on automated systems and networks, which can be disrupted if crews are unaware of the risks. By enhancing their understanding of cybersecurity practices, organizations can reduce vulnerabilities and maintain operational continuity during a cyber incident.

Another key recommendation is to publish policies that adequately cover critical areas of maritime cybersecurity. Kanwal et al. (2022) argue that policies must address essential aspects such as system readiness, training, and monitoring requirements. Policies provide a framework for implementing cybersecurity measures, ensuring organizations remain proactive in addressing potential risks. By setting clear training, system maintenance, and incident response guidelines, policies help standardize cybersecurity practices across the maritime sector.

Furthermore, the chart stresses the need for a cybersecurity company strategy aligned with organizational goals. Kala and Balakrishnan (2019) emphasize that companies should integrate cybersecurity into their broader strategies. This includes running crew performance measurements, assessing value delivery, and effectively implementing security measures. Aligning cybersecurity strategies with organizational objectives ensures that security becomes a priority rather than an afterthought, fostering a coordinated and systematic approach to tackling cyber risks.

Finally, the recommendation to use contemporary examples of cyber-attacks in training programs highlights the importance of practical, real-world learning. Hareide et al. (2008) suggest that training sessions incorporate case studies and actual cyber-attack examples to enhance the navigators' competence and system awareness. By examining past incidents, seafarers can better understand the nature of cyber threats, learn how systems can be exploited, and develop strategies to prevent similar attacks in the future. This approach enhances critical thinking and ensures crews are equipped to handle complex cybersecurity challenges.

In conclusion, raising seafarers' cybersecurity awareness requires a multi-faceted approach involving training, policies, and strategic alignment. Proper and regular training helps employees and crews effectively identify, prevent, and respond to cyber threats. Policies provide a structured framework for addressing critical areas of cybersecurity while aligning cybersecurity strategies with organizational goals to ensure a systematic approach to risk management. Incorporating real-world examples into training further enhances awareness and preparedness. Together, these measures are vital in strengthening cybersecurity in maritime operations, ensuring safer and more resilient shipping systems.

## Conclusions.

Maritime cybersecurity has become an especially critical issue both nationally and internationally. Seafarers' awareness of cyber security in shipping operations must be maintained.

It can be concluded that Malaysian seafarers are not fully aware that a lack of organizational framework can be a factor in organizational cyberattacks. However, they agree and are aware of other factors, such as no proper training, connectivity, the converging of IT & OT, and the infection of malware and ransomware. The respondents agree that outdated software is the most influential factor in cyberattacks. The early hypothesis is based on research from Canepa et al. (2021), as they conclude that the lack of awareness is true. The results of the study are to evaluate seafarers' level of awareness of cyberattacks in shipping operations.

The contributions of this research are to propose recommendations to raise seafarers' level of awareness of cyber security in shipping operations. Even though a few maritime organizations and companies have made many efforts to raise awareness of cyber security, its effectiveness might not achieve its target. The data from this research can contribute to any institution or organization in the maritime field to improve cyber security in shipping operations in Malaysia.

**Acknowledgements.**

We sincerely thank the University of Malaysia Terengganu and the maritime cyber security experts who generously participated in the interviews. Their insights into the field proved to be invaluable.

**References.**

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

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

Ashraf, I. Park, Y. Hur, S. Kim, S.W. Alroobaea, R. Zikria, Y.B. and Nosheen, S. (2022) A survey on cyber security threats in iot-enabled maritime industry. IEEE Transactions on Intelligent Transportation Systems. 24(2). p.2677-2690.

Canepa, M. Ballini, F. Dalaklis, D. and Vakili, S. (2021) Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain. In INTED2021 Proceedings. p. 3489-3499.

Det Norske Veritas (DNV) (2023) Digitalization in the maritime industry. [Online] Available from: https://www.dnv.com/-maritime/insights/topics/digitalization-in-the-maritime-industry/-index.html [Accessed: 11/12/2023].

Hanzu-Pazara, R. Raicu, G. and Zagan, R. (2019) November. The impact of human behaviour on cyber security of the maritime systems. In Advanced Engineering Forum 34 p. 267-274.

Hareide, O.S. Jøsok, Ø. Lund, M.S., Ostnes, R. and Helkala, K. (2018) Enhancing navigator competence by demonstrating maritime cyber security. The Journal of Navigation. 71(5). p.1025-1039.

Hopcraft, R. and Martin, K.M. (2018) Effective maritime cybersecurity regulation–the case for a cyber code. Journal of the Indian Ocean Region. 14(3), p.354-366.

International Maritime Organization (IMO) (2019) Maritime Cyber Risk. Available from: https://www.imo.org/en/OurWork/-Security/Pages/Cyber-security.aspx [Accessed: 22/10/2023].

Kanwal, K. Shi, W. Kontovas, C. Yang, Z. and Chang, C.H. (2022) Maritime cybersecurity: are onboard systems ready? Maritime Policy & Management. p.1-19.

Lagouvardou, S. (2018) Maritime Cyber Security: concepts, problems and models. Kongens Lyngby, Copenhagen. p 19-28.

Lee, Y.C. Park, S.K. Lee, W.K. and Kang, J. (2017) Improving cyber security awareness in maritime transport: A way forward. Journal of Advanced Marine Engineering and Technology (JAMET). 41(8), p.738-745.

Meland, P.H. Bernsmed, K. Wille, E. Rødseth, Ø.J. and Nesheim, D.A. (2021) A retrospective analysis of maritime cyber security incidents.