International Journal of Information Security
https://doi.org/10.1007/s10207-024-00884-2

REGULAR CONTRIBUTION

Survey-based analysis of cybersecurity awareness of Turkish seafarers

Ivar Moen[1] · **Aybars Oruc**[1] · **Ahmed Amro**[1] · **Vasileios Gkioulos**[1] · **Georgios Kavallieratos**[1]

Abstract

In recent years, vessels have become increasingly digitized, reflecting broader societal trends. As a result, maritime operations have become an attractive target for cyber threat actors. Despite the limited cybersecurity training seafarers receive, they are expected to operate within technologically advanced environments. The importance of cybersecurity awareness is evident, but the extent of seafarers' knowledge in this area remains uncertain. This article investigates three primary aspects: (1) the current state of cybersecurity onboard cargo vessels, (2) seafarers' cybersecurity awareness, and (3) potential improvements in seafarers' cybersecurity awareness. To accomplish this, a literature review is conducted to collect and analyze current research, supplemented by a questionnaire survey targeting Turkish seafarers. Our findings support increased investment in awareness and training programs, including organizational-wide cybersecurity awareness efforts, more frequent training, mandatory training for all seafarers through the Standards of Training Certification and Watchkeeping (STCW), and the appointment of a cybersecurity Officer (CySO) to ensure satisfactory cybersecurity levels onboard. Since this article focuses on high-level topics by assessing the general state of maritime cybersecurity and seafarers' cybersecurity awareness, it does not delve into detailed considerations of awareness and training programs. Nevertheless, it lays the foundation for future research in this area.

Keywords Maritime · Cybersecurity · Training · Awareness · Questionnaire

1 Introduction

In the contemporary global economy, maritime transport serves as the backbone of international trade, handling nearly all global transportation of goods [3, 4]. This pivotal sector serves as critical infrastructure, underpinning economic prosperity and facilitating the distribution of indispensable commodities [40]. As we advance into an era of digital transformation, vessels have evolved into complex technological ecosystems, incorporating state-of-the-art information technology (IT) and operational technology (OT) systems [9, 22]. These sophisticated systems steer navigational procedures, enhance intra-ship communication, support vessel safety measures, and monitor cargo and ballast management, heralding limitless possibilities for future maritime operations.

Yet, as these systems become more intricate, the potential for cybersecurity threats increases, particularly when the primary operators of these systems, the seafarers, often lack formal IT training [32]. Despite their extensive maritime expertise, seafarers are typically not equipped with robust cybersecurity skills, a predicament highlighted by critics of maritime education programs [24, 49]. Given this discrepancy, the question arises: How can we ensure secure vessel operations when the majority of onboard personnel may not have adequate cybersecurity knowledge?

Historical digitization trends have revealed that human errors consistently pose a significant cybersecurity threat, often due to inadequate user awareness [76]. As digital environments become more complex, the likelihood of such human-induced errors and their subsequent impact on system security increases [23]. Therefore, understanding the state of cybersecurity awareness among seafarers is a critical first step toward identifying potential vulnerabilities and instituting effective preventive measures.

Recognizing the profound implications of ongoing digital transformations, the maritime industry has called for extensive research into maritime cybersecurity to ensure reliable and secure operations [62]. In response to this call, our research addresses three primary research questions:

✉ Ahmed Amro
ahmed.amro@ntnu.no

[1] Norwegian University of Science and Technology (NTNU), Gjøvik 2815, Norway

Published online: 10 July 2024

- What is the current state of cybersecurity onboard vessels?
- What is the level of cybersecurity awareness among seafarers?
- How can we enhance cybersecurity awareness among seafarers?

These questions guide our research focus toward understanding the present cybersecurity landscape onboard cargo vessels and assessing the cybersecurity awareness of seafarers. We deliberately exclude passenger vessels from our research to eliminate the unpredictable variable of passenger behaviour, which could compromise cybersecurity onboard. Additionally, despite the increasing interest in autonomous vessels, our research does not delve into their cybersecurity issues, as our primary interest lies in human interaction with computer systems.

Our research is concentrated on security issues rather than safety concerns, focusing on the prevention of harmful actions, unauthorized data access, or manipulation of information. Data for our research was collected through a questionnaire survey distributed among seafarers affiliated with two maritime organizations in Turkey. Although our sample is region-specific, the findings may hold value for the global maritime community, given the sector's international character.

The remainder of this article is organized as follows: Sect. 2 establishes the theoretical background necessary to understand the field of maritime cybersecurity in general and the cybersecurity awareness of seafarers in particular. Section 3 present related research and situates these within the context of this article. Section 4 describes the methodology used to design and conduct the questionnaire survey. Section 5 presents results from the data collection done in the questionnaire survey and analyzes the results. Section 6 discusses the results from the questionnaire and proposes improvements to maritime cybersecurity awareness following the research questions, questionnaire data, and literature review. Section 7 concludes the article, discusses its limitations, and proposes future work.

2 Background

2.1 Maritime cybersecurity

To understand how maritime cybersecurity can be improved, it is important to first be aware of its current state, including technical, organizational, and operational aspects. This section seeks to establish a general description of maritime cybersecurity.

2.1.1 Organizational elements of the vessel

Vessels, for this article, will be considered primarily within the context of cargo transportation. They come in various forms, each tailored to transport specific types of cargo such as tankers, container vessels, roll-on/roll-off (RORO) vessels and dry cargo vessels. The differences between these are not further explored in this article.

The hierarchical structure of a vessel consists of the management, operational, and support levels [32]. The management level includes the Master, also known as the Captain, who commands the ship, as well as senior officers such as the Chief Officer, Chief Engineer, and Second Engineer [58]. Junior officers, including the Officer on Watch, Engineer Officer on Watch, or Electro Technical Officer, constitute the operational level. The support level consists of ratings, which form part of a navigational or engine watches, or catering services. It is worth noting that the roles and ranks may vary based on the specific vessel and company.

2.1.2 Current state of cybersecurity in the maritime sector

The rapid surge in digitization has escalated the need for robust security measures in computer systems susceptible to attacks. The proliferation of digital systems amplifies the risk profile, providing cybercriminals with an expansive playground to exploit [39].

In the maritime sector, cybersecurity developments display varying degrees of sophistication, depending on the analytical lens applied. A school of thought argues that maritime cybersecurity is deficient, primarily due to the absence of comprehensive cybersecurity policies embedded in vessel procedures and protocols [69, 72, 73]). This gap in integrating cybersecurity components within overarching vessel safety protocols is believed to negatively impact the overall security posture. Counterarguments emphasize the necessity of a holistic approach to cybersecurity, balancing technical interventions with human-centric considerations [41]. Human decision-making processes are subjective and prone to biases, factors that potentially influence cybersecurity incidents. However, the maritime industry appears to have overlooked the human dimension of cybersecurity [41].

Amid these challenges, there are promising aspects of maritime cybersecurity. Oruc [53] assessed the cybersecurity implications of vetting programs used for vessel risk assessment, such as Ship Inspection Report Programme (SIRE) and Tanker Management and Self-Assessment (TMSA), highlighting the positive impact of including cybersecurity queries in the vetting process. The International Maritime Organization's (IMO) 2017 resolution mandated the inclusion of cybersecurity elements in the Safety Management Systems (SMS) of vessels by January 1st, 2021 [28, 30]. Oruc's research found that the tanker industry initiated these processes, indicating a focus on cybersecurity in certain maritime segments.

Yet, the IMO resolution is the only official international document outlining cybersecurity prerequisites for its Member States [2, 27]. Critics argue that countries' efforts to combat cybercrime at sea are inadequate, suggesting an overall deficiency in cybersecurity attention. However, more recent studies, such as [34], indicate that some maritime companies have developed cybersecurity procedures within their safety management systems, indicating a positive response to the 2021 IMO requirements.

Studies have also highlighted the correlation between managerial attitudes towards cybersecurity and organizational security outcomes. Avanesova et al. [5] found that while Chief Information Officers invested in technical security, they overlooked measures to enhance cybersecurity awareness. Jensen [33] further corroborated the lack of understanding of cyber threats at the managerial level, emphasizing the necessity of international cybersecurity guidelines for the maritime sector.

Progoulakis et al. [59] assessed cybersecurity within the offshore oil and gas sector, pointing out a similar lack of comprehension among senior executives. They argued that without a clear understanding of cybersecurity concepts and threats, it is unlikely that implementation of effective cybersecurity measures will be prioritized. This underscores the crucial role top-level management plays in bolstering the overall security of an organization.

2.1.3 Current state of cybersecurity in vessels

Modern shipping vessels are equipped with a variety of intricate systems designed to facilitate safe and efficient operations. Some essential systems on the bridge include Global Navigation Satellite System (GNSS), Electronic Chart Display and Information System (ECDIS), external communication systems (e.g., satellite communication and internet services), main propulsion control units, and ship monitoring and security systems (e.g. Ship Security Alert System (SSAS)) [38]. While these systems are indispensable, they are also rife with potential vulnerabilities.

As ben Farah et al. [21] have noted, the rising dependence on the internet, unprotected computers, and a lack of appropriate security training for crews greatly heighten the risk of successful cyber attacks. A prominent challenge is the plethora of different IT and OT systems onboard, resulting in a complicated ecosystem. Despite this complexity, there appears to be a greater emphasis on physical security over cybersecurity regarding these critical systems [59].

Navigational devices such as the GNSS, ECDIS, and Automatic Identification System (AIS) are crucial for efficient and safe navigation. However, these systems are susceptible to malicious interference since these systems rely on communicating with external systems (e.g. sattelites) to function.

For example, the AIS provides real-time information about a vessel's position and movements but lacks encryption mechanisms, leaving it open to data manipulation or misinformation campaigns [21]. Similarly, GNSS uses sattelites to calculate positioning data. This makes it possibly for threat actors to intercept the communication between vessels and the sattelites, and deliver false positioning data to the vessels [6, 44]. As described by Leite Junior et al. [43] it is even possible to intercept AIS and ECDIS communication as a back door for sending commands that trigger cyber attacks in other information systems onboard the vessel.

Many vessels use Very Small Aperture Terminals (VSAT) for communication between the vessel and land. While this makes it possible for vessels to have a sattelite broadband connection, it might also expose them to unnecessary threats. As with other maritime communications technologies, VSAT is dependent on transferring data to sattelite receivers far away, but it lacks encryption mechanisms that secures the data [55]. As a result of this, confidential communication can be exposed to threat actors equipped with necessary tools for conducting eavesdropping activities.

Ben Farah et al. [21] argue that the surge in digitization is leading to an increase in system vulnerabilities, particularly in Internet of Things (IoT) devices due to their web-based cloud connections. If attackers were to exploit an onboard IoT device, other critical systems could be compromised [67].

Another concern lies in the outdated technology often found in older vessels, which frequently have outdated computer systems not designed with a cybersecurity focus. Implementing modern cybersecurity measures within these vessels poses a significant challenge [25, 26].

Multiple studies by Svilicic et al. have found that computer systems onboard vessels are not updated frequently, leaving them exposed to potential cyber threats. A reason might be a lack of specific cybersecurity policies and procedures onboard [69–73]. In [72] Svilicic et al. highlight that maritime vessels are primarily dependent on digital tools for navigation, essentially sailing without analogue alternatives. Given that vessels rely this heavily on digital tools for navigation, it underscores the critical need for robust infrastructure that address the inherent vulnerabilities of these technologies.

2.1.4 Cyber threats to maritime operations

To comprehend the threat landscape in the maritime sector, it is necessary to understand the various threat actors involved. The Baltic and International Maritime Council (BIMCO) [9] classifies these threats into targeted and untargeted attacks, with actors ranging from accidental malware spreaders to nation-states conducting deliberate attacks.

Various governmental agencies and private organizations regularly publish threat assessments to aid public and private organizations in bolstering their cyber defences. For example, the Center for cybersecurity (CFCS) in Denmark has identified a high threat from cyber attacks towards navigational systems used in maritime operations [13]. Similarly, the Norwegian organization NORMA Cyber has noted a range of actors targeting international maritime operations, including nation-states and cybercriminals [51].

Threat actors in the maritime sector could also include terrorists, pirates, activists, spies, and even employees within the vessel posing as an insider threat. A wide variety of cyber attacks have been reported in the maritime sector, demonstrating the broad range of attacks that the sector is currently facing. Examples include manipulation of positional AIS data of a vessel, injection of malware through unsolicited emails or distribution of malware through IoT devices.

2.2 Cybersecurity awareness and training of seafarers

The preceding sections highlighted the current state of cybersecurity within the maritime industry. Of particular interest is the fundamental role that seafarers, and their interaction with computer systems, play in ensuring secure and efficient operations of vessels. This section, therefore, delves into the elements of cybersecurity awareness and training among seafarers.

McGillivary [46] postulates that ship crew and management often find themselves at a loss in case of a cybersecurity breach. Although a stark statement, it resonates with a significant proportion of the industry. Studies by researchers such as Bolat and Kayişoğlu [10], Alcaide and Llave [1], Mraković and Vojinović [49], and Senarak [64, 65] reveal a pervasive lack of cybersecurity awareness among maritime personnel. Research also underscores the relationship between the level of cybersecurity training among seafarers and vessel safety [25]. Furthermore, a deficit in cybersecurity awareness could also expose vessels to physical attacks in addition to digital ones. Karahalios [36] reported that poor cybersecurity awareness rendered vessels more susceptible to digitally savvy pirates, particularly in piracy-prone waters.

Addressing this knowledge gap naturally points to enhancing training. Despite the critical role of cybersecurity, it often receives inadequate attention in the maritime industry. The International Convention on Standard of Training, Certification and Watchkeeping for Seafarers (STCW), which lays the foundation for most maritime training, does not explicitly mention cybersecurity. However, the increasing recognition of the importance of cybersecurity training is reflected in organizations providing such training, possibly fueled by the IMO's Resolution MSC.428(98) [18].

It is uncertain how many enrol in such courses or programs. Based on the lack of cybersecurity focus in the sector, it is probable that the engagement is lower than necessary. However, some credited maritime organizations such as the Oil Companies International Marine Forum (OCIMF), heightened their cybersecurity efforts already before the implementation of the IMO's resolution.

2.3 Improving the state of maritime cybersecurity awareness

The contemporary landscape of cybersecurity underscores a pressing need for an elevated level of cybersecurity awareness. Many researchers have proposed various measures intended to improve the state of cybersecurity in the maritime sector. Some argue that it is important to incorporate cybersecurity awareness in all levels of the organization, and that effort should begin from the top [2, 37, 48, 59]. Extensive scholarly discourse suggests the necessity for a widespread and organizational approach to cybersecurity awareness, commencing from executive management down to the operational levels [5]. This approach, mainly aiming to secure the top management's commitment, is pivotal for adequate funding allocation, strategic planning, and setting the organization's trajectory.

Nonetheless, the promotion of comprehensive organizational involvement in cybersecurity awareness programs is inadequate alone. It is crucial to account for personal factors such as cultural distinctions. Research by Karamperidis et al [37], highlights cultural differences between European and Asian cultures and how they shape our perspectives on and responses to cyber risks. This indicates that one training approach that works sufficiently in one geography or culture is not necessarily perfect for another, and makes it important to not forget that people from different cultures have different ways of thinking.

Risk perception, influenced by individual knowledge of threats, and IT and OT systems' functionality, also plays a significant role in shaping cybersecurity measures [41]. Therefore, training initiatives should be personalized to align with specific employee roles, vessel activities, and challenges they face [66, 67]. For instance, onshore employees likely experience different cybersecurity challenges compared to their onboard colleagues [59, 64, 65].

Meanwhile, the maritime industry would benefit from enhanced regulatory standards or guidelines [36]. This could involve strengthening the role of the IMO to develop and enforce comprehensive measures, regulations, and guidelines that combat cyber threats [2]. Furthermore, integrating cybersecurity training into the mandatory elements of the STCW is envisioned to contribute to improving digital competencies in cyber risk management practices [25].

In addition to the above, redesigning organizational roles may prove beneficial. For instance by introducing a CySO responsible for safeguarding the overall cybersecurity state of the vessel and the entire organization [11]. These recommendations, originating from the extensive cybersecurity research body, demonstrate how minor adjustments could yield significant improvements to maritime security.

One step to improving the overall awareness is to educate both specialists and generalists in maritime cybersecurity. Nikolov discusses how to address new challenges of maritime cybersecurity education and highlights the importance of having a curriculum aimed at both management level and technical level [50]. Here, he underlines that technical courses should contain sufficient curriculum regarding IT and OT of ship systems so that these can be protected properly. Similar views are presented in [15] that discusses a course on cybersecurity in maritime industrial control systems that was taught at the U. S. Naval Academy.

However, cybersecurity is not only the responsibility of IT personnel, but all employees within the company. This implies that training should include all personnel, whether they are seafarers, general office workers or IT specialists. As discussed by Erstad et al. [19], this can be done by not only educating seafarers individually, but including stakeholders from a broader part of the maritime supply chain in simulations and trainings. Another approach is the one presented in [54] where a modular cybersecurity training programme is introduced. Such a modular approach can make it easier to fit the training programme to a varied group of people and their roles within the company.

3 Related work

A literature review is essential for a structured search, selection, analysis, and comparison of scientific literature, and serves as the basis of background information discussed in this article.

To maintain thoroughness and minimize bias, Okoli's [52] steps for conducting literature reviews were adapted for this research. This simplified approach consists of five steps: identification of purpose, literature search and selection, data extraction and quality appraisal, data synthesis, and writing the review.

3.1 Stages of literature review

In the first step, the purpose of the literature review was defined. That is to locate, analyze, and discuss literature related to maritime cybersecurity, helping to answer three primary research questions.

The second step involved literature search and selection. A strategy was formulated to identify research papers that could answer the research questions, focusing on search engines, search strings, and inclusion/exclusion criteria. Oria, Web of Science, and Engineering Village were the chosen search engines. The search strings used were "maritime cybersecurity", "maritime cybersecurity awareness", "maritime cybersecurity training", "maritime cyber risks", and "maritime cyber threats". Papers had to be peer-reviewed, written in English, and discuss maritime cybersecurity. They also needed to be published by acknowledged organizations or institutions.

The search generated 559 hits, from which 35 papers were selected for initial screening. To maintain an overview, information about the papers was documented separately.

In the third step, data extraction and quality appraisal took place. Relevant information was extracted from the papers based on the research questions. Each paper was carefully read, and notes were written in a separate document. The papers were graded based on their relevance to the research questions. Twenty-nine papers were considered highly relevant, four somewhat relevant, and two less relevant.

The fourth step involved data synthesis. Literature was grouped according to topics and viewpoints corresponding to the relevant research question.

Lastly, the review was written, as presented here. It was additionally used to answer research questions in Sect. 6. Although the selection, grading and evaluation of research papers were subjective and influenced by biases, this literature review approach was designed to be comprehensive, thorough, and minimize bias, with the ultimate goal of providing a strong foundation for understanding maritime cybersecurity awareness.

3.2 Overview of related studies

Alcaide and Llave [1] conducted research on the cybersecurity knowledge of maritime professionals by distributing an online questionnaire to a large number of potential participants. In total, the questionnaire received 124 responses, but only 102 were analysed. The researchers pointed to poor network connectivity onboard vessels being one reason why they were able to collect what they considered few participants, but also that many recipients likely saw the email invitations as spam or similar.

In total, the questionnaire consisted of 14 questions, including demographic questions and more specific questions related to cybersecurity knowledge. The researchers highlight that 33% of the participants answered that they had experienced a cyber incident within the last year, 40% stated that they share passwords with colleagues, and in general that the cybersecurity knowledge of maritime personnel is too poor. They also found that many seem to focus on technical cybersecurity measures without focusing enough on the human element in cyber risk. Additionally, they stress that technical cybersecurity is not enough to protect the maritime sector, but that cybersecurity training is important to achieve sufficient security levels.

Mraković and Vojinović conducted a study to assess the level of cybersecurity awareness of seafarers [49]. This was done using a questionnaire distributed to active seafarers in Montenegro. Out of a total population of 3,000, they gathered a sample of 429 participants who all had officer ranks.

The questionnaire consisted of 18 questions that were based on various cyber threats and best practices. To assess the level of cybersecurity awareness of the participants, they applied ISRAM; the Information Security Risk Analysis Method [35], to calculate a risk value using a certain formula. Using this method gave results indicating a medium risk level pointing to a poor level of cybersecurity awareness.

To improve awareness, Mraković and Vojinović proposed a training course that they believe should be mandatory for all seafarers onboard a vessel. This proposal includes repeating the course every five years and including it in IMO's existing security awareness training.

Bolat and Kayişoğlu conducted research to assess the effect of various measures on the cybersecurity awareness of Turkish seafarers [10]. This was done by conducting a questionnaire targeting officers and engineers working either onboard a vessel or onshore with at least one year of experience. They successfully collected responses from 211 unique participants in a target population of 15,000 people. The questionnaire consisted of 37 statements with Likert scale alternatives. The questions were divided into groups with topics such as cybersecurity awareness, secure user behaviour, cybersecurity education, and cybersecurity policies. During analysis, structural equation modelling (SEM) and exploratory factor analysis (EFA) were used to measure the effect of the different question groups concerning each other.

The analysis showed that education is an important factor in improving cybersecurity awareness, that knowledge of cybersecurity incidents affects awareness, and that cybersecurity awareness affects what level of cyber hygiene the participant has. At the same time, the analysis indicates that cybersecurity rules and policies have no significant effect on cybersecurity hygiene. The same applies to information-sharing practices. In essence, their findings confirm that cybersecurity education is an important part of raising the level of awareness.

4 Methodology

This section describes the questionnaire methodology used and the ethical considerations applied during the research.

4.1 Questionnaire methodology

The questionnaire for this research was developed using a methodology framework described by multiple renowned scholars, including Lee [42], Saris and Gallhofer [63], and Burgess [12]. The structural approach proposed by Burgess [12] served as the primary guideline. The seven key stages outlined by Burgess - defining research aims, identifying population and sample, deciding on the method of response collection, designing the questionnaire, conducting a pilot survey, implementing the main survey, and analyzing the data - were meticulously followed in this research.

The first step, defining research aims, centred on assessing cybersecurity awareness, personal and professional cybersecurity etiquette, and the depth of cybersecurity knowledge among the respondents.

The second step, identifying the population and sample, involved targeting Turkish maritime professionals, both active seafarers and office personnel with seafarer backgrounds. The total count of Turkish seafarers was approximately 28,000 in 2021 [29]. The targeted professionals were mostly registered with two Turkish maritime education websites managed by the co-author of this article, Aybars Oruc. To maintain the focus on the target population, control questions were inserted in the questionnaire to filter out respondents without relevant seafaring experience.

Given the size of the population, full-scale participation was not feasible or necessary. A representative sample suffices to make inferential statements about the population. Decisions regarding sample size were based on acceptable levels of sampling error (±5%), confidence level (95%), and variability measures. Previous related studies [10, 49] offered a benchmark to determine these parameters.

The third step is related to response collection. The survey was administered through the University of Oslo's Nettskjema tool. Email addresses were collected to maintain the uniqueness of responses, but they were later removed to preserve respondents' privacy. Further details on these processes are elaborated upon in the subsequent sections.

The fourth step involves designing the questionnaire. During the construction of the survey instrument, meticulous care was given to crafting questions that were explicit, purpose-driven, and comprehensible to the respondents, following Lee's guidelines [42]. The survey predominantly utilized closed-ended queries to expedite participant response and simplify subsequent data analysis. Limitations of this approach, such as potential participant confusion or misinterpretation of questions, were acknowledged and mitigated in the questionnaire design.

The survey consisted of 27 questions which were asked in four different styles, ranging from binary options (yes

Table 1 Date range for distribution of emails and the number of answers generated

Date range	Number of email recipients	Number of opened emails	Number of click on link	Number of questionnaire answers
September 9 to 14	40,758	2886	135	15
September 18 to 23	40,772	3661	151	29
September 26 to 29	40,811	3786	142	27
October 9 to 12	40,885	2223	108	46
Total number answers				117

or no) to multiple-choice queries. These questions aimed to measure aspects such as the respondents' background, their perceptions about cyber hygiene and awareness, and their understanding of different cybersecurity scenarios. Care was taken to ensure these questions were relevant to the overarching research objective.

The questions were also designed to validate the participant's experience as a seafarer, a criterion essential for this study's target demographic. The inspiration for the questionnaire came from previous research, including da Veiga's work on Information Security Culture Assessment (ISCA) [16, 17, 45], although da Veiga's methodology was adapted to align with the specific needs of this article.

Before distribution, the questionnaire was translated into Turkish to improve participant understanding and ensure data collection from the target demographic.

The fifth step consists of executing a pilot survey. The questionnaire underwent a continuous refinement process. A pilot survey was carried out with a Turkish-speaking maritime professional to test the questionnaire's coherence and the accuracy of the Turkish translation.

The sixth step is related to the execution of the main survey. The survey was distributed over five weeks in September and October 2022 to recipients on various mailing lists. Detailed records of email distribution, including the number of emails opened and links clicked, were maintained. Table 1 shows the time frames in which emails were sent out, the number of opened emails, and the number of links clicked as well as how many answers were gathered from each distribution sequence.

The seventh step is related to data analysis. The collected data, obtained from Nettskjema, were analyzed using IBM SPSS Statistics. Data preprocessing included combining smaller groups into larger ones and converting string variables to numerical variables with labels to facilitate more streamlined analysis. The primary analytical focus included descriptive statistics, data distribution, visual dependencies, and Analysis of Variance (ANOVA) tests, supplemented by Post hoc tests such as Tukey's Honestly Significant Difference (HSD) [56] and Fisher's Least Significant Difference (LSD) [57]. The threshold for statistical significance was set at "$p < 0.05$" as this is the generally accepted value to show statistically significant differences in the data [7]. This p-value is the likelihood that the same results will be achieved as long as the null hypothesis (H0) is true [61]. The H0 is essentially a hypothesis stating that the variables have no effect on the outcome, and the alternative hypothesis (H1) is the opposite. For the ANOVA tests, H0 indicates that there is no difference in group means [68].

4.2 Ethical considerations

The data collection process began after receiving approval from the Norwegian Agency for Shared Services in Education and Research (Sikt), validating the data collection and data management plan. Participation in the questionnaire was in its entirety voluntary, and the informed consent of participants was obtained through an invitation letter and a subsequent summary of it.

The questionnaire itself did not contain questions that would gather personal or identifiable information. Email addresses were however collected within the questionnaire platform to preserve the uniqueness of the responses. After ensuring the uniqueness of responses, email addresses were removed from the data and never used for analysis.

5 Results and analysis

This section presents the findings of the questionnaire and analyses the results. The data were analysed particularly for the population sample and confidence level, demographic data, personal perception of cybersecurity topics, and behaviour in given cybersecurity scenarios.

5.1 Population sample and confidence level

A total of 117 answers were initially received. After conducting a control process to ensure the uniqueness of responses, 115 unique answers were identified. In the questionnaire, two demographic questions were implemented to ensure the inclusion of participants with maritime experience only. Upon analysis, five participants were found to have provided responses indicating a lack of maritime experience or incoherent answers, leading to their exclusion from further analysis. Consequently, the final count of responses utilized in the research was 110. The resulting confidence interval of ±9.52% at a 95% confidence level, as calculated using Yamane's formula [77], was deemed a fair representation of the total population of 28,000 seafarers. This was considered acceptable given the scope of this article.

5.2 Demographic data

This section presents demographic data collected from 110 respondents based on several of the questionnaire questions. It aims to describe the background of the sample population.

The distribution of years of maritime experience and the participants' rank is shown in Fig. 1 and Fig. 2 respectively. It shows that most of the participants had significant experience in the maritime sector, and the majority had senior officer rankings.

When asked what type of vessel the participants worked on in their last contract, the majority answered dry cargo vessels and tankers, as shown in Fig. 3. Although the focus of this article is cargo vessels, the responses from the other groups are included in the analysis as their experiences from being seafarers in the maritime sector are likely relevant.

Participants were asked to provide information about their educational background. To balance out the fragmentation in the participants' responses, the educational levels were distinguished into three categories. The mapping of the new categories and their relevant old categories are depicted in Table 2. The distribution of answers according to the new categories of educational level is shown in Fig. 4. It appears that the majority of the participants pertain to high educational levels.

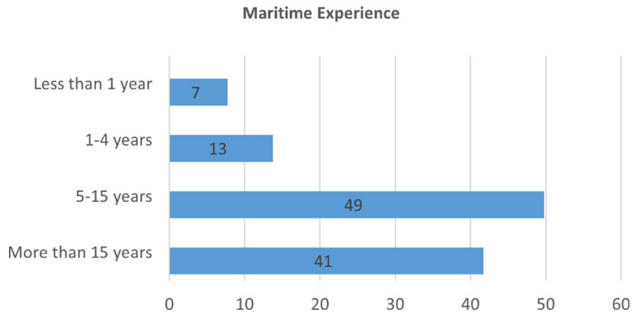

Fig. 1 Participants' maritime experiences

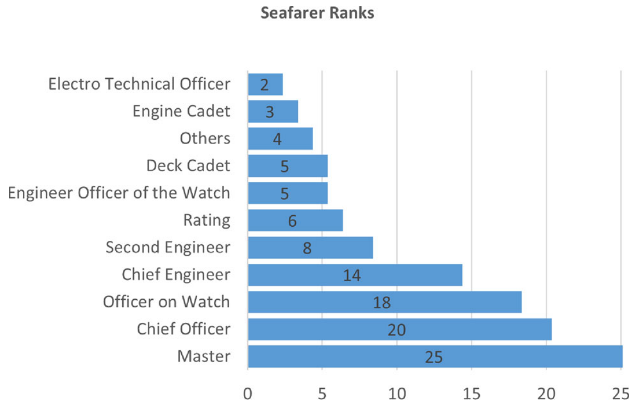

Fig. 2 Participants' seafarer ranks

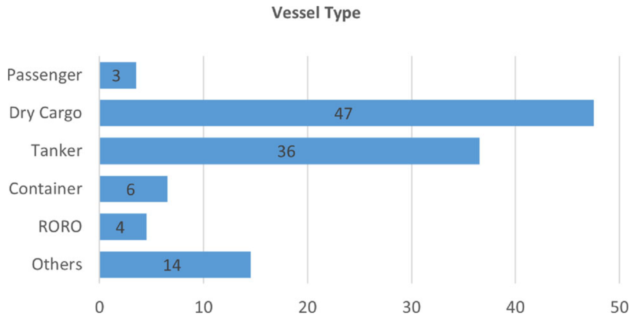

Fig. 3 Participants' vessel types in their last contract

Participants were asked if they had any formal education or training in information technology or cybersecurity. This question allowed the participant to tick all the applicable boxes, making the number of answers larger than the number of participants. The options include "No education", "Formal education from college/university", "Short courses taken in private", "Short courses through the workplace", and "Other types of formal education". To make the data more usable in analysis, the data were transformed to suit a binary format with the category "No education" staying the same, while all other categories were combined in a new category called "Education". The distribution shows that 65.5% (N = 72) of participants had some form of education or training in cybersecurity or IT, while 34.5% (N = 38) had none.

The participants were asked to grade their understanding of computers. Since it is natural to assume that having education in cybersecurity or IT increases the participant's computer understanding, these two variables were combined and illustrated in Fig. 5. The distribution indicates that most of the participants answered that their computer understanding is either very good or good, also have education in cybersecurity or IT.

One-way ANOVA tests were conducted to reveal the statistical significance of the computer knowledge assessment with the other demographic variables. The tests revealed that "Education in cybersecurity or IT" has a highly statistically significant difference in the group means, and implies that there is a relationship between the variable and its effect on the question.

Table 2 Overview of new education categories

New Category	Old Category
High school or lower	Secondary school, Vocational training, High school (non-maritime), and Maritime high school
Higher education from college	Vocational college (non-maritime), Maritime college
Higher education with academic degree	Bachelor's degree (maritime), Bachelor's degree (non-maritime), Master's degree, Doctor's degree (PhD)

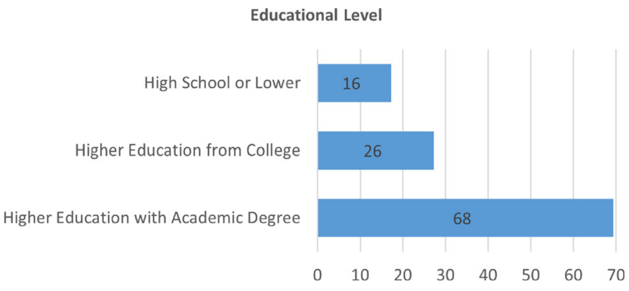

Fig. 4 Participants' education levels

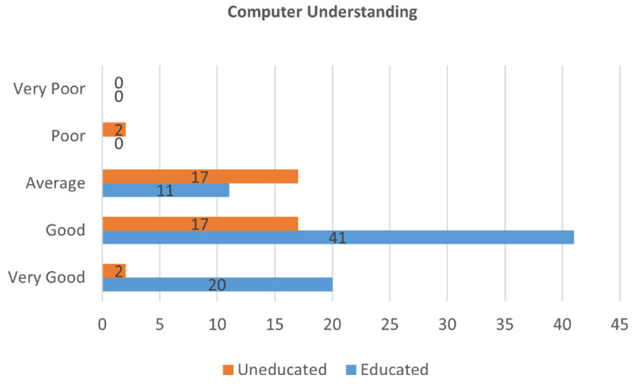

Fig. 5 Participants' computer understanding and education in cybersecurity or IT

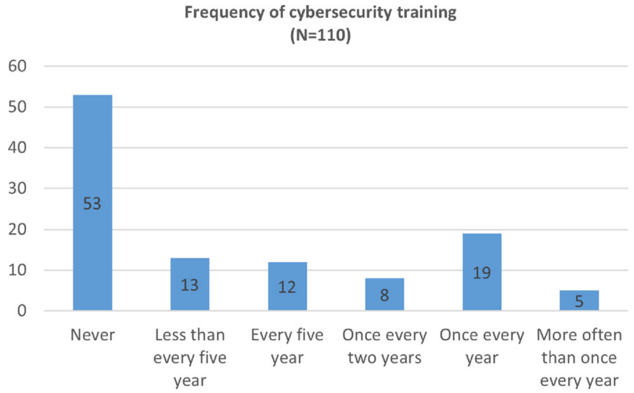

Fig. 6 Overview of frequency of cybersecurity training

5.3 Personal perception of cybersecurity

This section presents results from questions related to personal perception of cybersecurity. Different aspects of cybersecurity are assessed together to facilitate the presentation of the results.

5.3.1 Frequency of cybersecurity training

The frequency of the cybersecurity training was explored among participants. The goal was to reveal information about the daily routines and habits. The distribution, as depicted in Fig. 6, shows that 48.2% (N = 53) never receive cybersecurity training, 11.8% (N = 13) receive training less than every five years, 10.9% (N = 12) receive it every five years, 7.3% (N = 8) every two years, 17.3% (N = 19) once every year, and 4.5% (N = 5) more often than once every year. The majority of the participants claimed that they never received cybersecurity training while only 17.3% received training more than once per year.

To examine potential statistically significant differences in responses due to a selection of variables, several one-way ANOVA tests were conducted. The resulting p-values are presented in Table 3. The tests showed that only the variables "Type of vessel" ($p = 0.004$) and "Education in cybersecurity or IT" ($p < 0.001$) had p-values lower than the threshold of $p < 0.05$, indicating statistically significant differences in the group means. The variable "Type of vessel" exhibited significant differences between "Dry cargo" and "Tanker", and "Tanker" and "Other vessels", with "Tanker" participants indicating a higher frequency of cybersecurity training. Further, participants with an education in "cybersecurity or IT" were also found to have more frequent cybersecurity training. The remaining variables, "Maritime rank", "Years of maritime experience", and "Highest education level" showed no statistically significant difference in responses.

5.3.2 Preference in cybersecurity training

Several forms of cybersecurity training were presented to identify the most preferred among the participants. As presented in Fig. 7, 1.8% (N = 2) stated that they do not need cybersecurity training, 18.2% (N = 20) preferred in-person training, 32.7% (N = 36) preferred online training, while 4.5% (N = 5) of the responders chose remote training. The majority of the participants, 42.7% (N = 47), preferred a

Table 3 Results from one-way ANOVA test for cybersecurity training frequency

Variable	p-value
Maritime rank	0.687
Type of vessel	0.004
Years of maritime experience	0.110
Highest education level	0.354
Education in cybersecurity or IT	<0.001

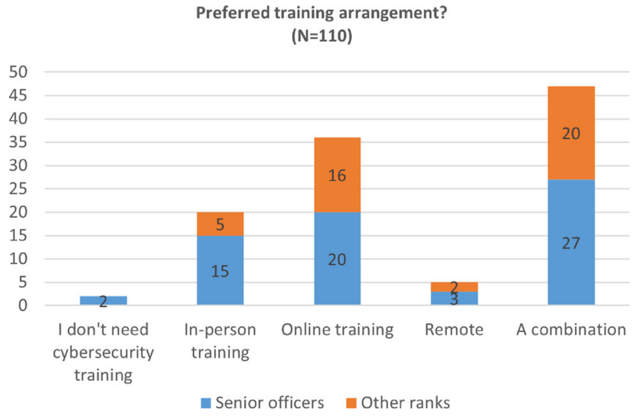

Fig. 7 Overview of preferred cybersecurity training with maritime rank

combination of self-study, in-person and online training. To illustrate whether there is a relation between the variables, maritime rank is considered in the analysis of the preferred training arrangements in Fig. 7. The distribution indicates that two senior officers answered that there is no need for cybersecurity training, while the rest of the distribution looks fairly equal in terms of maritime ranks. An exception occurs for in-person training where there seems to be a higher number of "Senior officers" preferring it. The daily interaction with the system functions and operations could influence the preference for cybersecurity training.

The one-way ANOVA tests revealed a statistical significance for the effect of "Highest educational level" (F(2,107) = [4.235], p = 0.017), with p-value $<$ 0.05. This implies that there is a relationship between the variables and their effect on the question. Because the variable involves several groups, post hoc tests using Tukey's HSD were conducted. These revealed that there is a statistically significant difference between "Higher education with academic degree" and "Higher education from college", (p = 0.015, 95% C.I. = [−1.46, −0.13]. There is no statistically significant difference between "Higher education with academic degree" and "High school or lower" (p = 1.000), or "Higher education from college" and "High school or lower" (p = 0.101). The tests indicate that what kind of educational level the participant has affects what kind of cybersecurity training arrangement they prefer. There also seems to be a preference for a combination of self-study, in-person training, and online training.

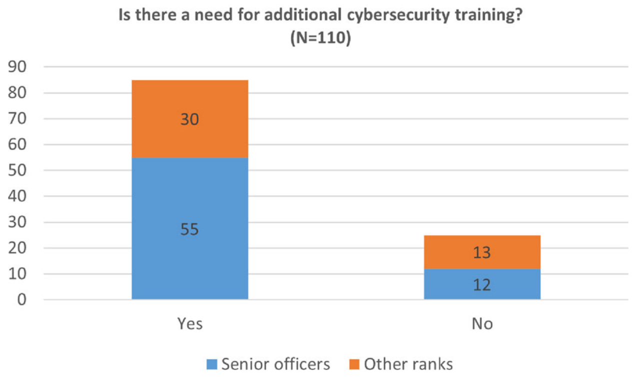

Fig. 8 Overview of need for cybersecurity training with maritime rank

5.3.3 Need for more cybersecurity training

A question intended to identify whether the current cybersecurity training is appropriate or whether there are need for improvements was asked. As depicted in Fig. 8, 77.3% (N = 85) of the participants identify that there is a need for additional cybersecurity training, and 22.7% (N = 25) answered that there is no need for any additional training. Looking at the distributions depicted in Fig. 8, the majority of "Senior officers" 82.1% (N = 55) answered "Yes", while 17.9% (N = 12) answered "No". Within the "Other ranks", 69.8% (N = 30) answered "Yes" and 30.2% (N = 13) answered "No". There seems to be a slightly larger percentage of "Senior officers" that find a need for additional cybersecurity training than "Other ranks". Although there seems to be a visual relationship between maritime rank and the participant's answer to whether or not there is a need for more cybersecurity training, the one-way ANOVA tests reveal that there is no statistically significant relationship. This also implies that any tendencies are due to chance. None of the other variables seem to affect participants' answers either. Overall, the distribution of answers illustrates that most of the participants believe there is a need for additional cybersecurity training in their workplace.

5.3.4 Mandatory cybersecurity training

Participants were asked whether or not they believe there is a need to make cybersecurity training mandatory as part of the STCW. The distribution in Fig. 9 illustrates that 60.0% (N = 66) answered "Yes", while 40.0% (N = 44) answered "No". In general, the effect of educational level is interesting to assess concerning this question. Two stacked bar charts involving the question about STCW with "Education in cybersecurity or IT" and "Highest educational level" were created. Visually,

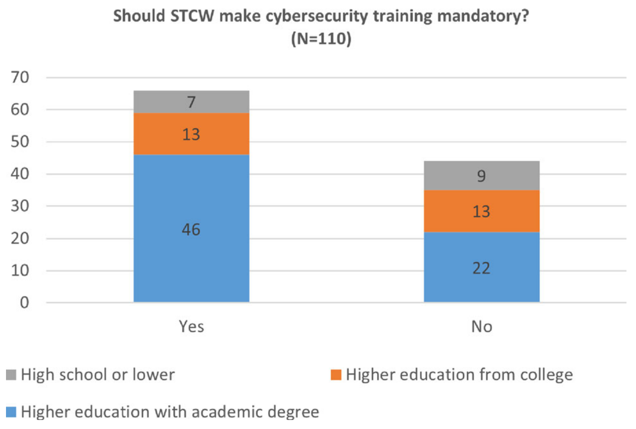

Fig. 9 Overview of cybersecurity training being mandatory with educational level

there seems to be a relationship between answering “Yes” to cybersecurity training being mandatory, and having either education in cybersecurity or having higher education with an academic degree.

After conducting one-way ANOVA tests, the only effect with a marginal statistically significant difference in the group means is the effect of “Education in cybersecurity or IT” (F(1,108) = [3.927], p = 0.050) with p-value = 0.05. This implies that there is likely some kind of relationship between having cybersecurity education and attitudes towards training being mandatory. Based on the distribution, having cybersecurity education makes it slightly more likely that the participant believes cybersecurity training should be mandatory through the STCW convention.

5.3.5 Senior crew’s attitude towards cybersecurity training

The contribution and importance of cybersecurity in the safety of the vessel are also explored in the questionnaire. Particularly, whether cybersecurity appears important for senior crew such as the master, chief engineer, chief officer, and 2nd Engineer. Figure 10 shows that 51.8% (N = 57) answered “Yes”, while 48.2% (N = 53) answered “No”. This indicates that there is a relatively equal distribution among the sample population. Moreover, taking into consideration the maritime ranks of the participants, 56.7% (N = 38) of “Senior officers” answered “Yes”, while 43.3% (N = 29) answered “No”. For “Other ranks”, the distribution was 44.2% (N = 19) at “Yes” and 55.8% (N = 24) at “No”. This indicates that there is a slightly higher number of “Senior officers” who believe cybersecurity is important for senior crew such as themselves. However, to test the effect of maritime rank on the belief that cybersecurity is important to the senior crew, a one-way ANOVA test was used. The test gave p = 0.203 (which constitutes p > 0.05). This indicates that there is no statistically significant difference in means between the maritime ranks and their beliefs related to how senior crew views cybersecurity. Although a few more participants answered that they believe the senior crew finds cybersecurity important, the difference is too small to conduct any generalization. There does not seem to be any significant difference in the demographic groups in terms of what they believe the senior crew thinks of cybersecurity.

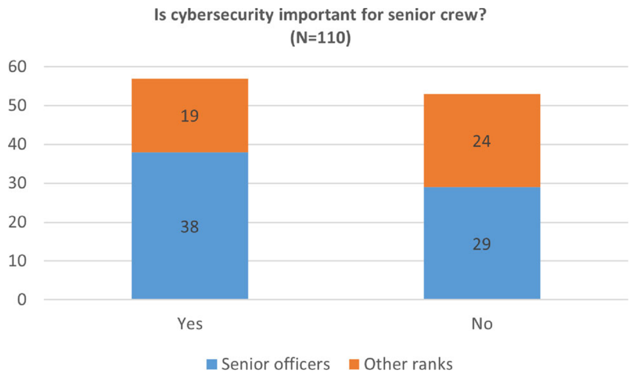

Fig. 10 Maritime ranks with beliefs about senior crew’s attitude

5.3.6 Knowledge of cybersecurity breaches

The awareness of participants regarding whether their company had faced any cyber attacks in the last 12 months was assessed. 1.8% (N = 2) of the participants answered “Yes”, while 98.2% (N = 108) answered “No”. When it comes to physical security breaches, 4.5% (N = 5) of the participants answered “Yes”, while 95.5% (N = 105) answered “No”. This indicates a slightly similar distribution regardless of what domain the security breach took place in. However, the number of participants who have experienced any kind of security breach is very low.

5.3.7 Knowledge of cybersecurity threats

The overall awareness related to cyber threats is considered in the next set of questions. Figure 11 illustrates that 90.0% (N = 99) answered that they are aware of cyber threats, while 10.0% (N = 11) answered that they are not aware. This indicates that a great majority of the participants believe they have some sort of awareness related to cyber threats. When looking at cyber threat awareness together with whether the participant has undergone any cybersecurity or IT education, the distribution indicates that there is a clear tendency in responses. Although the number of participants answering “No” is low, most of whom have done so also state that they have no education in cybersecurity or IT. Similarly, a higher number of participants answering “Yes” to cyber threat awareness also say that they have some kind of cybersecurity education. Carrying out a one-sided ANOVA

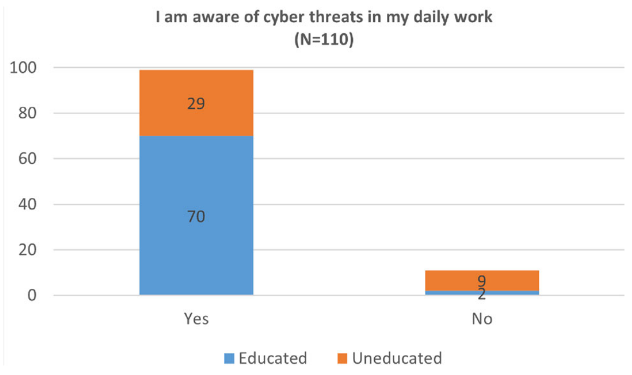

Fig. 11 Overview of cyber threat awareness with cybersecurity education

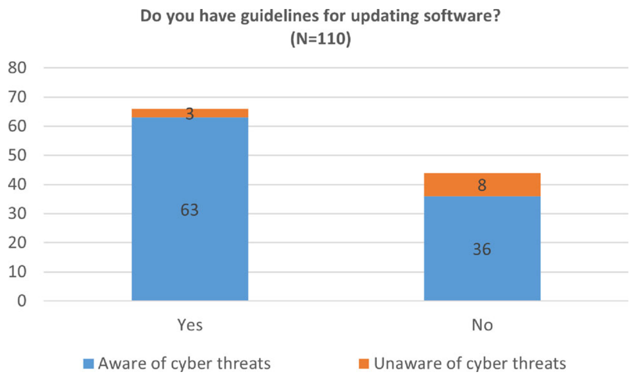

Fig. 12 Overview of software updating guidelines with cyber threat awareness

test on the effect of cybersecurity education on cyber threat awareness gives a p $<$ 0.001, since (F(1,108) = [13.323], p $<$ 0.001). This means that there is a statistically significant difference in the answers indicating that knowledge of cybersecurity threats is related to whether the participant has any education in cybersecurity or IT.

5.3.8 Guidelines for updating vessel navigation systems

When asked whether there are any existing guidelines and policies related to regular updates of navigational systems such as Multifunction Display (MFD), ECDIS, and Radio Detection And Ranging (RADAR), the majority of the participants, 60.0% (N = 66), indicated that there are guidelines in place while 40.0% (N = 44) answered that there are none. Similarly, the existence of guidelines for software, operating systems, and antivirus updates onboard the vessel is explored. 55.5% (N = 61) of the responders answered "Yes" and 44.5% (N = 49) answered "No". This indicates a discrepancy between the two questions. Table 4 shows that participants answering "Yes" to one question did not necessarily answer "Yes" to the other, indicating an irregularity between guidelines and practices.

Focusing on the guidelines, it is interesting to look at the relationship between software updating guidelines and cyber threat awareness. These variables are illustrated in Fig. 12. While the number of participants answering "No" to whether they are aware of cyber threats in their daily work is quite low, there seems to be a higher percentage of these participants also answering "No" to having software updating guidelines onboard. When carrying out a one-way ANOVA to test the effect of software updating guidelines on participants' cyber threat awareness, the test gives p $<$ 0.05 since (F(1,108) = [5.635], p = 0.019). This indicates that there is a statistically significant difference in the answers, which implies that whether software updating guidelines exist might affect cyber threat awareness of the personnel onboard vessels.

More one-way ANOVA tests were conducted to test the effect of other variables on how the participant responded on having software update guidelines. For the variable "Education in cybersecurity or IT", we can conclude that there is a likely relationship between whether the participant has any education in cybersecurity and how they responded to the question as the p-value indicates a marginal statistically significant effect, (F(1,108) = [3.927], p = 0.050). The distribution indicates that having cybersecurity education makes it more likely that they also have guidelines for updating software. For "Type of vessel", the test indicates that the variable has a significant effect on what answer is chosen (F(2,107) = [3.763], p = 0.026). Because the variable involves several groups, post hoc tests using Tukey's HSD were conducted. These revealed that there is a marginal statistically significant difference between "Tanker" and "Other vessels", (p = 0.045, 95 % C.I. = [0.01, 0.59]. There is no statistically significant difference between "Tanker" and "Dry cargo" (p = 0.058) or "Dry cargo" and "Other vessels" (p = 0.901). The tests indicate that what type of vessel the participant last worked on might affect whether they answered that their

Table 4 Crosstabulation of software updating guidelines with actual practice

		Is computer software updated regularly?		Total
		Yes	No	
Do you have guidelines for updating software?	Yes	45	21	66
	No	16	28	44
Total		61	49	110

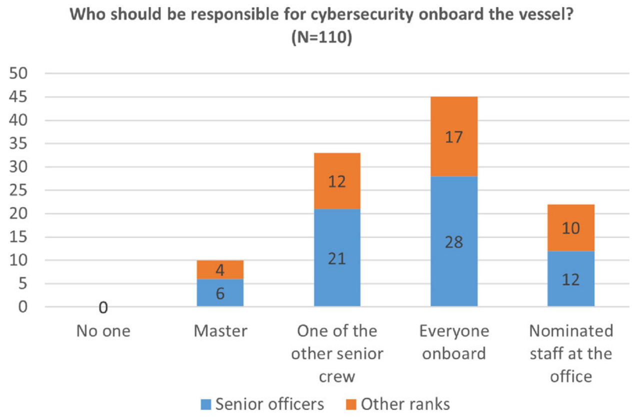

Fig. 13 Maritime rank with opinions on cybersecurity responsible

company has guidelines for updating navigation system software, with participants from tanker vessels having the highest chance of answering that they have such guidelines. Similarly, having education in cybersecurity or IT also seems to influence the responses. Lastly, there seems to be a connection between having software updating guidelines and being aware of cyber threats in their daily work.

5.3.9 Responsible for cybersecurity onboard vessels

The cybersecurity accountability onboard the vessel is explored through the questionnaire. Particularly, the participants were asked to indicate what role/rank is responsible for the cybersecurity of a vessel. The distribution in Fig. 13 depicts that 9.1% (N = 10) answered "Master", and 30.0% (N = 33) answered "One of the other senior crew". The majority of the responders, 40.9% (N = 45), answered "Everyone onboard", and 20.0% (N = 22) answered "Nominated staff at the office". None of the participants answered "No one". A significant number of the participants answered "Everyone onboard", and when looking at the answers compared to what maritime rank the participant has, it looks like the distribution is relatively equal between the groups. 41.8% (N = 28) of the "Senior officers" believe everyone on board is responsible for cybersecurity, while 39.5% (N = 17) of "Other ranks" believe the same. Similar tendencies are seen for the other alternatives. For instance, 17.9% (N = 12) of "Senior officers" believe that nominated staff at the office should be responsible, while 23.3% (N = 10) from "Other ranks" believe the same. The rest of the distribution is presented below.

Although none of the demographic variables indicates a statistically significant effect on who the participant believes is responsible for cybersecurity, the general distribution indicates that many participants believe everyone onboard shares the responsibility. The second largest group believes that it is the responsibility of one of the senior crew, but not the master. This indicates that participants disagree on who is responsible for cybersecurity onboard vessels.

5.4 Behavior in cybersecurity scenarios

The questionnaire contained questions aimed at assessing the participants' behaviour in cybersecurity scenarios. These were intended to help assess participants' knowledge of cybersecurity-related topics, as described in Sect. 4 on methodology. All questions had four alternatives, but not necessarily one correct answer. Where relevant, this is specified for each scenario below and further discussed in Sect. 6.

5.4.1 Scenario 1: someone asks for the wifi password

"Someone at the port asks you for the password to the vessel's wifi. How do you respond?" The distribution presented in Table 5 shows that almost all (88.2%, N = 97) answered alternative 3 "You refuse to share the password and immediately notify your superior." One could likely argue that this is the preferred answer. It is also worth noting that a total of 6.4% (N = 7) answered that they would share the WiFi password in one way or another, while 5.5% (N = 6) answered: "You refuse to share the password, but log in the person's device so that he or she can get access to the WiFi anyways". Without having any decisive solution, one could likely argue that alternatives 1, 2, and 4 are less desirable than number 3. This means that while almost all participants answered "You refuse to share the password and immediately notify your superior", there is no statistical evidence supporting differences between the groups. Additionally, 11.8% of participants answered the less desirable alternatives.

5.4.2 Scenario 2: you receive an email about outdated antivirus

"You receive an email that tells you the vessel's antivirus is outdated and tells you to update it by clicking the attachment. How should you react?" In this question, none of the participants answered alternative 1 "You follow the instructions of the email and click the attachment to install the update". The rest of the distribution is presented in Table 6. There is not necessarily a right answer, but both alternatives 2 "You get suspicious of the email and report it to the IT department" and 4 "You ignore the instructions of the email and delete it" likely constitute preferable answers. Depending on the actions of the supervisor, alternative 3 "You show the email to your supervisor and ask them to check the attachment for you" could in theory also be acceptable.

The one-way ANOVA tests revealed that there is likely a difference in answers depending on what type of vessel the participant is coming from, with effects related to "Dry cargo" and "Tanker" vessels. The tests also reveal that having

Table 5 Answers to scenario question 1 (N = 110)

Alternative	N	%
Check the reason for asking and share the password	6	5.5%
Share the password without asking why	1	0.9%
Refuse to share and notify superior	97	88.2%
Refuse to share, but log into the person's device	6	5.5%

Table 6 Answers to scenario question 2 (N = 110)

Alternative	N	%
Get suspicious and report to IT	59	53.6%
Show the email to a supervisor and ask them to check the attachments	16	14.5%
Ignore email	35	31.8%

Table 7 Answers to scenario question 3 (N = 110)

Alternatives		N	%
1	Reuse old password	4	3.6%
2	Use same password as colleague	3	2.7%
3	Create new password based on the old	15	13.6%
4	Create a totally new password	88	80.0%

Table 8 Answers to scenario question 4 (N = 110)

	Alternatives	N	%
1	Ignore email and delete it	24	21.8%
2	Report email to supervisor	73	66.4%
3	Answer email and tell to contact someone else	12	10.9%
4	Answer email and explain security routines	1	0.9%

education in cybersecurity or IT makes it more likely that the participants answered that they would get suspicious of the email and report it to IT.

5.4.3 Scenario 3: you need to update your old password

"When logging into a computer you are asked to update the password because the old one has expired. What should you do?" The responses are shown in Table 7. In this question, most of the participants (80.0%, N = 88) answered alternative 4. The second highest group, being significantly smaller, answered alternative 3. The remaining 6.3% (N = 7) answered either alternative 1 or alternative 2. Although there are no definitive correct answers to this question, the two first alternatives are the least correct answers, alternative 4 is likely the most correct answer, and alternative 3 is somewhere in between.

A series of one-way ANOVA tests were conducted to evaluate the influence of various variables on participants' responses in a given scenario. The results showed that most variables did not significantly affect the answers, with the exceptions being "Type of vessel" and "Education in cybersecurity or IT". A significant correlation was found between participants with cybersecurity or IT education and a propensity to create entirely new passwords ($p < 0.001$). The type of vessel also influenced responses, specifically those working on tanker vessels were more likely to choose to create a new password compared to those on dry cargo vessels ($p = 0.037$). Post hoc analysis revealed no significant difference in responses among other vessel types. Overall, participants were more likely to create new passwords, but education in cybersecurity or IT, and working on a tanker vessel, increased this likelihood.

5.4.4 Scenario 4: an email asks about the vessel's security routines

"You receive an email from someone asking you for details about vessel security routines. How do you react?" The distribution as depicted in Table 8 shows that 21.8% (N = 24) answered alternative 1. Also, (N = 73) answered alternative 2. The remaining 11.8% (N = 13) answered either alternative 3 or alternative 4. Similar to the other scenarios, there are not necessarily correct answers here. However, one could likely argue that alternatives 1 and 2 are the most correct, and alternatives 3 and 4 are the least correct. This is further discussed in Sect. 6.

No statistically significant difference was found between the various groups in terms of what they answered to the scenario. The distribution reveals that most of the participants answered one of the alternatives that included not replying to the email, but a total of 11.8% of participants answered the least correct alternatives.

5.4.5 Scenario 5: you find a USB memory stick

"While walking into the vessel, you find a USB memory stick. What do you do?" The distribution in Table 9 shows

Table 9 Answers to scenario question 5 (N = 110)

	Alternatives	N	%
1	Leave the USB alone	2	1.8%
2	Pick up USB and put into vessel computer	3	2.7%
3	Pick up USB and put into private computer	8	7.3%
4	Inform supervisor about USB	97	88.2%

Table 10 Answers to scenario question 6 (N = 110)

	Alternatives	N	%
1	Write on paper and attach to device	6	5.5%
2	Remember password in own mind	13	11.8%
3	Write in dedicated list in vessel	78	70.9%
4	Write electronically and store in computer	13	11.8%

that 1.8% (N = 2) answered alternative 1 and 88.2% (N = 97) answered alternative 4. The remaining 10.0% (N = 11) answered either alternative 2 or alternative 3. In this scenario, one could argue that the most correct alternatives involve not inserting the USB memory stick into any computer. We can therefore state that alternatives 1 and 4 are the most correct, and alternatives 2 and 3 are the least correct.

Even though none of the variables had any statistically significant effect on the responses to the scenario, we can conclude that most of the participants answered that they would either leave the USB alone or report it to a superior. A total of 10% answered that they would insert the USB into a computer to check the contents.

5.4.6 Scenario 6: Where do you store passwords to computer systems?

"You are asked to change the password for the ECDIS, GPS, purifier or similar, how do you store the password?" The distribution in Table 10 shows that 70.9% (N = 78) answered alternative 3. For the other participants, 5.5% (N = 6) answered alternative 1, 11.8% (N = 13) alternative 2, and 11.8% (N = 13) alternative 4. This scenario has alternatives representing various degrees of best practice. A recognized best practice stated in BIMCO's guide [8] is to have a dedicated list of passwords for vessel computer systems onboard the vessel. The guide also indicates that writing the password electronically and storing it on a computer (with restricted access) is also accepted. However, writing it on paper and attaching it to the device is not recommended. Having that in mind, alternatives 3 and 4 are likely the most correct. One could also argue that alternative 2 is adequate as it limits the likelihood of the password getting into the hands of someone unauthorized. Alternative 1 is the least correct.

Since none of the variables seem to have a statistically significant effect on the way participants answered in the scenario, no generalization on the grounds of demographic backgrounds can be made. However, the general distribution shows that most of the participants would store the password in a dedicated list in the vessel. At the same time, 5.5% answered the least correct answer.

6 Discussion

This section proposes measures to enhance seafarers' cybersecurity awareness based on the analysis results.

Out of 115 unique answers, 110 were analyzed since they were from seafarers with maritime experience. The majority had 5–15 years of experience, while the second largest group had over 15 years. Senior officers comprised 60.9% of maritime ranks, the remaining were lower ranks. Dry cargo vessels had the most participants, followed by tanker vessels. The remaining employees worked in vessels not mentioned, like RORO, container, and passenger. Almost all participants held an academic or college degree, as only 14.5% of participants had a high school or lower education level. 65.5% of participants had education in cybersecurity or IT, including formal and shorter courses from work or privately. When asked, most participants rated their computer knowledge as good or higher, with only two rating it as poor.

6.1 Cybersecurity perception

The data regarding specific cybersecurity-related topics suggest that the overall state of cybersecurity awareness is slightly better than for the studies described in the background section.

6.1.1 Cybersecurity awareness

Most participants had work-related cybersecurity awareness, with 90% recognizing cyber threats, and awareness of cyber threats was associated with education in cybersecurity or IT. This indicates that having cybersecurity education also makes the person more aware of cyber threats in their daily work. While not unexpected given the topics covered in the background section, it is still important to note this correlation. Participants in the research showed awareness of cyber threats in their daily work, despite prior research indicating inadequate levels of cybersecurity awareness. However, the participants cannot specify known cyber threats due to the question's breadth. Furthermore, it is worth stating that education in cybersecurity correlates with a good computer understanding. Thus, having a good understanding of computers is likely a great benefit when considering cybersecurity awareness.

Participants were asked about physical and cybersecurity breaches within their company's vessels in the last year. 1.8% reported knowing a cybersecurity breach, while 4.5% knew of a physical breach, indicating that barely anyone was familiar with either kind of breach. Several factors may have caused this low number. Ideally, few participants claiming to know of a breach would indicate a low number of actual incidents. However, this topic is discussed in the limitations section, as it may arise from reluctance to disclose compromising information about their workplace, or information about incidents may not reach participants on all vessels. Assuming truthful responses, the low number of incidents is positive.

6.1.2 Cybersecurity training

Almost half of the participants never receive cybersecurity training, while the other half receive training with some frequency. The high number of participants without cybersecurity training is alarming. It is, however, not surprising when having in mind that few regulations or frameworks have made such training mandatory. Resolution MSC.428(98) is a step in the right direction, with Guidelines on Maritime Cyber Risk Management effective from January 1st, 2021 [28]. This makes it mandatory to include cyber risks in the safety management systems but does not specify that cybersecurity training should be mandatory. The number of untrained participants suggests the resolution had little impact on cybersecurity training. One important, and possibly easy, improvement would therefore be to conduct cybersecurity training more frequently, as cyber threats evolve with technology, requiring updated knowledge to combat them.

Cybersecurity training frequency varies based on vessel type, with tanker vessels having a more frequent training regime than others. Section 2 discusses how this may be linked to specific requirements for tanker, such as those outlined by the OCIMF in 2017. The TMSA 3 mandates member vessels to include cybersecurity awareness in the overall training of seafarers. Regardless of vessel type, maritime rank, or experience, 69.8% of participants believe that more cybersecurity training is necessary, indicating a desire for additional cybersecurity training across the entire population.

Given the majority's interest in more cybersecurity training, adapting the training arrangements to participants' preferences is imperative. Online and blended training is preferred by most participants, while the answers indicate that diversity in cybersecurity training is advantageous. cybersecurity training is most engaging when participants have the freedom to choose. Online training is typically structured so that the participant can complete training material within a set time frame but at their own pace. However, some people may favour traditional classrooms and interact with teachers in person, and it may be prudent to allow seafarers the freedom to choose their training.

While the STCW convention [31] requires seafarers to receive in-depth training in various aspects of vessel safety and security, it does not mandate obligatory cybersecurity training, as noted in Sect. 2. In response to whether cybersecurity training should be mandatory for seafarers through the STCW, 60% answered "yes". Interestingly enough, most respondents had some form of prior cybersecurity education. This might imply that having a basic understanding of cybersecurity principles makes it clear how important correct cyber hygiene is for maritime operations. Despite majority support, a significant portion of participants oppose mandatory cybersecurity. The participant's answer lacked elaboration, leaving the reasons unclear and varied. Some might find it challenging to have more mandatory training, but would still choose to undergo cybersecurity training voluntarily. However, to ensure that cybersecurity is taken seriously in all organizations, it could be wise to make it a mandatory requirement as part of the STCW as proposed by others [25]. This way, the regulatory framework would enforce a minimum of cybersecurity awareness in training programs.

6.1.3 Attitude towards cybersecurity

Approximately 50% of the participants think that cybersecurity training is needed for the senior crew, and this is not influenced by maritime rank, indicating that cybersecurity is likely not as high on the agenda as it should be. As discussed in Sect. 2, other researchers have argued that cybersecurity should be implemented in the whole organization for it to be effective [2, 37, 48, 59]. Despite not being part of onshore top-level management, senior crew onboard vessels are the highest level of management onboard. Their perspectives and opinions impact daily operations, including their attitude towards cybersecurity and its integration into work. The data suggests that there is room for improving the cybersecurity attitude of senior crew onboard vessels.

Participants were also asked who should be responsible for cybersecurity on a vessel. 40.9% said everyone is responsible, 9.1% said the master is responsible, and 30% said a senior officer is responsible. Overseeing certain tasks onboard is normally the responsibility of senior officers. It is therefore not surprising that many have answered this. Interestingly, 20% believed that nominated staff at the office should be responsible.

These answers suggest that some participants believe cybersecurity is not their responsibility. Thus, assigning one person to oversee cybersecurity on the vessel is wise, despite everyone onboard being familiar with and following cybersecurity principles. It is common for vessels to have multiple people assigned specific tasks. One possibility is to appoint a CySO, as suggested by the Institution of Engineering and Technology (IET) [11], who would then be in charge of maintaining a high level of cybersecurity onboard. Smaller vessels may have an onshore representative for fewer seafarers, maintaining the CySO role regardless of vessel size. The CySO would then have to make sure that seafarers are updated on cyber threats, that security guidelines exist and that best practices are being followed in daily operations.

6.1.4 Cybersecurity guidelines

The questionnaire also contained questions regarding vessel guidelines. cybersecurity guidelines on board, particularly those for securing vulnerable computer systems, were found to be lacking by Svilicic and other researchers [69, 71–73]. This is supported by Karahalios who also points to the lack of enforcement of guidelines as a vulnerability [36].

Participants were asked about company guidelines for updating vessel navigation systems, and whether computer systems onboard the vessel are updated regularly. Guidelines were reported by 60.0%, but only 55.5% update systems regularly. The two questions reveal a discrepancy: some do not follow updating guidelines and some update without guidelines. The low number of cases makes definitive conclusions difficult, yet it is interesting to mention. It might imply that having guidelines for updating systems is not enough, but that someone also has to make sure that they are being followed.

Despite the discrepancy, many participants do not have guidelines and do not update important software regularly. Despite the questionnaire's general nature, it confirms Svilicic's findings. Maritime organizations should enforce software update guidelines to secure against cyberattacks.

The data also suggests a link between cyber threat awareness and software updating guidelines. Mutual effects are possible, but software updating guidelines can enhance seafarers' awareness of cyber threats, and cyber threat awareness may enhance seafarers' understanding of software update guidelines. This applies to other variables as well, indicating the positive impacts of implementing cybersecurity measures onboard.

6.2 Cybersecurity scenarios

The scenario answers align with personal perception question findings. Most participants showed an understanding of cyber threats and maritime cybersecurity, but some answered oppositely indicating a need for improvement.

6.2.1 Scenario 1

In the first scenario, participants were asked "Someone at the port asks you for the password to the vessel's Wi-Fi. How do you respond?"

88.2% opted not to share the password, which was the correct answer as per section 4. The goal was to test the participant's awareness of social engineering, as the person asking could be someone with malign intentions. Unfortunately, 11.8% of participants were willing to share the Wi-Fi password or help the stranger log in. The last option was added to evaluate if the participant perceived any difference between sharing the password directly or granting Wi-Fi access in another manner. The problem with sharing Wi-Fi passwords is the access it grants to the vessel's Wi-Fi, not the password itself. Lack of concern about Wi-Fi security among some participants suggests a need for greater awareness.

6.2.2 Scenario 2

In the second scenario, participants were asked: "You receive an email that tells you the vessel's antivirus is outdated and tells you to update it by clicking the attachment. How should you react?"

A surprising difference in answer distribution was observed here. All participants showed situational awareness regarding suspicious emails as no one agreed to follow instructions. Still, 14.5% of participants indicated that they would ask their supervisor to double-check the attachment. The email could either be ignored or reported to the IT department according to the vessel's routines, with catastrophic or optimal results, depending on the supervisor's actions. It is uncertain why this many participants answered that they would show the email to the supervisor when 'cybersecurity awareness. This, however, can be attributed to the fact that on vessels, personnel hierarchy can limit decision-making authority as one moves down the ranks. If that's why, it is possible a participant would want to verify their actions with a supervisor. Providing proper guidelines can counteract this issue for seafarers dealing with such emails. As expected, those with a cybersecurity or IT education reported suspicious emails to IT. This highlights the significance of understanding fundamental cybersecurity principles and reinforces the necessity of providing cybersecurity education for seafarers.

6.2.3 Scenario 3

For the third scenario, participants were asked: "When logging into a computer you are asked to update the password because the old one has expired. What should you do?"

This article does not provide any specific solutions for creating passwords because they depend on multiple factors that differ from one organization to another. For example, The National Cybersecurity Agency of France released "Best practices for cybersecurity on board ships" [75]. Guidelines suggest strong passwords should not include identifiable information and should not be shared.

The questionnaire showed that 80% would create a significantly different password. This option is the best, as it reduces the risk of account misuse if old passwords fall into unauthorized hands. The high number of responses to this option suggests a good understanding of password policies, influenced by company policies, personal experiences, security knowledge, or other factors. Despite this, 20% of participants selected less favourable options, with many opting to generate a new password based on the previous one. The new password may be acceptable, but it is not recommended. However, reusing old passwords (3.6%) and using colleagues' passwords (2.7%) are both unacceptable. A lack of cybersecurity awareness is implied by this last option, which increases the possibility of unauthorized personnel accessing user accounts. Adopting multi-factor authentication (MFA) on vessel systems would be a useful countermeasure against password breach issues, with BIMCO recommending this measure [9].

6.2.4 Scenario 4

In scenario 4, the participants were asked: "You receive an email from someone asking you for details about vessel security routines. How do you react?"

The goal was to assess awareness of email dangers, including phishing and social engineering. The main priority is to not respond to the email, with 88.2% choosing to ignore or report it. Reporting the email could lead to IT department investigations and improve threat awareness. Thus, being the preferred alternative.

A small fraction of participants, 0.9%, said they would explain security routines via email. Nonetheless, 10.9% of the participants mentioned that they would answer the email and recommend the sender to reach out to someone else. The implication is that social engineering's role in cyber attacks should be given more attention to stress that viruses and hackers aren't the only threats. To prepare for unsolicited emails that may end up in a person's inbox, awareness programs should include real-life scenarios. Awareness programs with email hygiene best practices could enhance cybersecurity [49, 66, 67]. Furthermore, management should provide guidelines for handling suspicious emails.

6.2.5 Scenario 5

In the fifth scenario, participants were asked: "While walking into the vessel, you find a USB memory stick. What do you do?"

The goal was to test awareness of USB attack threats. 88.2% would report to their supervisor, with 1.8% opting not to touch it, with both alternatives being beneficial. According to [47], this attack vector has been employed in attacks on the maritime sector before.

It was surprising to find out that 10% would choose to insert the USB stick either into their personal computer or into a computer on the ship. These participants either lack knowledge of USB device-initiated attacks or are unaware of appropriate responses. The fact that most participants chose a beneficial answer is positive, but the presence of undesirable answers highlights the need to include these topics in awareness programs and guidelines.

6.2.6 Scenario 6

In the last scenario, the participants were asked: "You are asked to change the password for the ECDIS, GPS, purifier, or similar, how do you store the password?"

We aimed to evaluate the participant's knowledge of best practices or company guidelines. As an alternative to the best practice recommended by BIMCO [8], 70.9% opted for writing it down on a dedicated list stored in the vessel. Another option proposed by 11.8% of the participants is to write it down electronically and save it on the computer. BIMCO's best practices recommend this as an alternative, provided the file is encrypted to prevent unauthorized access.

It is worth noting that 5.5% of people chose to write the password down on paper and attach it to the computer. Luckily, vessels often have good physical security ensuring that few unauthorized people have access to secure areas [36]. Depending solely on physical security to prevent unauthorized access is not ideal. More emphasis should be placed on password management training to enhance awareness.

6.3 Improving the state of cybersecurity awareness

Improving cybersecurity awareness involves augmenting one's knowledge and grasp of cybersecurity. Contributing to someone's cybersecurity knowledge also boosts their cyber hygiene, which refers to all the measures taken to safeguard against threats. Good cyber hygiene can be seen as equivalent to good cybersecurity practices. Good cyber hygiene for this article is shown by seafarers following guidelines and best practices in their daily work. cybersecurity culture is a comparable term that has various meanings depending on the situation, but it generally refers to how a group or organization manages cybersecurity problems in their daily work [60].

Seafarers form a collective group of people in the maritime community. However, each company, vessel, or small group of employees may have a subculture of their own that influences daily behaviour. This in turn affects their cybersecurity culture. Without diving into aspects of maritime culture, it is important to state that this culture should allow for behaviour that supports a satisfactory level of cybersecurity.

Human behaviour affects cybersecurity, be it cyber hygiene or security culture, while improving this behaviour would enhance cybersecurity. Considering this, we need to revisit the research results. There was disagreement among participants on multiple aspects. They disagreed on cybersecurity responsibility, training amount, format, and requirements for seafarers. A considerable percentage of participants tended to select incorrect options for most of the scenario questions related to cybersecurity principles. However, when questioned directly, nearly all profess to know cyber threats in their daily work. The findings show that there is a range in participants' cybersecurity habits, suggesting room for improvement.

Based on the background and proposals of other researchers, our research supports the application of some improvements and additional measures:

- A requirement to undergo cybersecurity training as part of the STCW.
- More frequent cybersecurity training.
- Choice of cybersecurity training arrangements, including in-person, online, and self-study options.
- cybersecurity awareness training in all levels of the organization.
- An appointed person with the role of CySO to ensure an overall satisfactory level of cybersecurity onboard.
- Ensuring that all seafarers understand how and why common cybersecurity practices should be applied in daily work.

The suggested measures could assist in improving structural arrangements, however, related policies and awareness and training programs could also be improved. Certain important elements should be considered, supported by the findings of our research:

- A real-life focus on cyber threats and how they can affect seafarers in their daily work.
- Guidelines for updating vessel software and routines for ensuring that these are followed.
- Multi-factor authentication for computer systems onboard.
- Stronger password policies and efficient ways of ensuring that they are followed.
- Training programs that include the dangers of social engineering, and not only the threat from malware or other technical attacks.
- Information on how emails and USB devices can be misused by threat actors in cyber attacks.

While additional factors may be necessary for training and awareness programs, this should be reserved for further research. However, it is recommended to customize cybersecurity training based on the organization and the participants' roles. The use of generic training programs can be seen as uninteresting, impersonal, or irrelevant to the participant [14]. The proposal is to offer common fundamental courses for all seafarers, and various job-specific courses, to guarantee that each role is aware of the cyber threats and best practices linked to their domain. Furthermore, instead of presenting training and awareness programs as necessities, organizations should also strive to make them engaging and interesting. According to Corradini (2020), requiring participation without explaining could result in unenthusiastic employees who are not motivated to engage in the training.

Additionally, individual differences in risk perception must be acknowledged when designing training and awareness programs. Being human, individuals onboard tend to make mistakes [23], and human errors in onboard computer systems enable half of all maritime cyber attacks [20]. Without space for mistakes or open discussion, cybersecurity culture may suffer. However, mistakes can vary in severity, with some being capable of causing significant damage to the vessel. However, the maritime sector would benefit from having a culture where it is possible to be insecure about how to act correctly, where challenging topics can be discussed and where it is ok to ask questions in all security-related areas. Although today's case isn't necessarily dire, it is worth noting that promoting an open culture could make it easier for people to comprehend the intricate field of cybersecurity and potentially bolster cybersecurity awareness overall.

cybersecurity communication must take into account that not everyone is familiar with technical language, so we must make an effort to familiarize people with necessary aspects, in a way that is easily understandable for an average person. In general, as "people acquire adequate information and are familiar with it, they are more likely to develop a favourable attitude towards the content they have received" [14].

There is a difficulty in compiling a list of all the solutions that can aid in improving cybersecurity awareness. Despite various suggestions for improvement, none of them will solve all the maritime sector's issues quickly. However, the sector is being positively affected by every little improvement. An organization can choose to enhance training frequency and introduce cybersecurity awareness programs throughout the company without STCW enforcement, as what works for one maritime organization may not be effective for another.

6.4 Limitations

6.4.1 Sample size

The sample size gives a clear limitation to the findings of this research. Having only 110 participants in a total population of about 28,000 gives a relatively high margin of error with a confidence interval of 95%. However, as described in the methodology section, a lot of effort was put into recruiting participants for this questionnaire.

There were about 40,000 email recipients in each of the four distribution rounds. Here, between 2,223 and 3,786 opened the email each time. Only between 108 and 151 recipients clicked the link to the questionnaire, and between 15 and 46 answered the questionnaire each time. This indicates that although quite many received and opened the email, relatively few were willing to click the link. Even after clicking the link, many were reluctant to answer the questionnaire.

Why this happened is unknown, but could be related to scepticism of clicking a link in an unsolicited email, potential participants not understanding the reason to participate or potential participants not having the time to participate. Regardless of this, it is important to remember that the conclusions made above are limited and cannot necessarily be extrapolated to the whole population. The data does nevertheless give an insight into the population.

6.4.2 Nationality

This research focused on Turkish seafarers, meaning that seafarers from other nationalities were excluded. This provides an understanding of the specific group but is not necessarily transferable to seafarers of other nationalities. In various countries, cyber security is taught as a compulsory course during the undergraduate education of cadets. For instance, at Tallinn University of Technology's Estonian Maritime Academy, the Introduction to Cyber Security course [74] is mandatory for students in the navigation and ship engineering departments [54]. In this course, students are exposed to a curriculum customized for maritime cyber risks. However, to the best of our knowledge, undergraduate curricula in maritime education in Turkey do not include such a course. Therefore, the study is limited to Turkish seafarers, and research results may vary among seafarers of different nationalities. The article does not attempt to draw conclusions applicable to the entire maritime sector across different nationalities, but has narrowed the scope to include only Turkish nationals. This was done not only for practical purposes but also to remove uncertainties that could arise within the data from having participants from different nationalities.

6.4.3 Ship type

As detailed in Sect. 5.2, the majority of seafarers participating in our survey had experience on cargo ships (e.g., tankers, dry cargo ships, containers, and RORO vessels). There is a possibility that cyber security awareness of seafarers varies depending on the type of vessel. However, since most survey participants had experience on tankers and dry cargo ships, we do not have sufficient data to measure the impact of vessel type on cyber security awareness.

6.4.4 Statistical analysis

During the statistical analysis, only two variables were analyzed together at a time. This was done to systematically assess the relationships between important variables. Not conducting multivariate analysis might have led to some correlations being less visible.

The methodology did not include metrics that could be used to quantify the level of cybersecurity awareness amongst seafarers. This was instead qualitatively assessed based on established cybersecurity practices and the authors' knowledge of cybersecurity.

6.4.5 Demography

A significant part of the participants were senior officers and had extensive experience in the maritime sector. There were relatively few participants from lower ranks and with few years of experience. Additionally, there were more participants from tanker vessels and cargo vessels than from other vessel types.

6.4.6 Few pedagogical elements in the questionnaire

The article analyses the current state of cybersecurity awareness without exploring pedagocical elements explaining how cybersecurity awreness programs should be designed. Therefore, it does not explore exactly what constitutes best practices for teaching.

6.4.7 Willingness to answer truthfully

Some of the questions in the questionnaire contain topics that might be perceived as sensitive or difficult to answer for someone unwilling to compromise themselves or their company. It is possible that some participants are unwilling to report that they have been under a cyber attack or similar for fear of being identified.

6.4.8 Relatively wide scope of research

Because the article explores a diverse group of vessels and personnel, the scope of the research is relatively wide. Even though this has led to interesting findings, the article is limited to giving high-level recommendations as opposed to detailed improvements to awareness programs, training arrangements, or cybersecurity policies and guidelines.

6.5 Future research

There are numerous approaches to future research based on this article. Firstly, the community can benefit from conducting a similar research project with a larger sample size. Alternatively, the total population size could be reduced by narrowing the scope to fit selected groups in the maritime sector. This could lead to a smaller margin of error and findings that are even more applicable to the maritime sector in general.

The population could also be altered by focusing on other nationalities, not only Turkish seafarers, or be narrowed to only include specific vessel types. Future research could also assess if there are differences between passenger vessels and cargo vessels. Another approach would be to assess the differences in cybersecurity awareness across different populations, for instance, grouped according to maritime rank, vessel type, years of experience, or similar variables. As mentioned, a limitation of this project is that the collected data primarily comes from highly ranked maritime personnel. Future research should also attempt to look at how personnel from lower ranks relate to cybersecurity.

As this has been a study into cybersecurity awareness and training, without focusing on the pedagogical perspective, future research could explore how pedagogical factors affect cybersecurity awareness. A similar research project could also benefit from exploring what specific topics should be included in the awareness programs.

Lastly, a deeper exploration of cyber hygiene and cybersecurity culture in the maritime sector could be undertaken. As culture tends to differ between groups of people, it is valuable to understand more of what effects maritime culture has on the overall state of cybersecurity.

7 Conclusion

This research aimed to assess the current state of cybersecurity onboard vessels, the current state of cybersecurity awareness of seafarers, and how this awareness can be improved. This was done through a literature review diving into the state of the art on the field, and a questionnaire survey targeting Turkish seafarers.

Based on the literature review, the overall state of cybersecurity awareness in the maritime sector was found to be unsatisfactory. Awareness and training seem to be insufficiently prioritized amongst the senior management of maritime organizations, something that likely affects the overall effort put into it. Having few regulatory requirements and guidelines makes cybersecurity awareness and training less influential than efforts put into other areas of maritime security. Some argue that cybersecurity training should be mandatory as part of the STCW, and others argue that the position of the IMO should be strengthened with cybersecurity guidelines valid for a larger part of the maritime sector. The literature review does nevertheless highlight the fact that effort must be put into increasing the status of cybersecurity awareness and training to properly secure maritime operations.

By assessing and analyzing the participants' knowledge of cybersecurity principles and how they would act in given cybersecurity-related scenarios, a general understanding of their awareness level was acquired. This revealed that the overall awareness level is slightly better than anticipated through the literature review. There was also a significant difference for those having education in cybersecurity or IT, implying that such education is positive for the overall state of maritime cybersecurity. It did nevertheless reveal a substantial number of participants with a poorer knowledge than what is desired, indicating that effort should be made through cybersecurity training. However, with a slightly poorer confidence level than desired together with a sample population consisting of mostly senior officers with many years of maritime experience, and a higher academic education, it is likely that the data is not representative of all Turkish seafarers.

The findings from the research give an insight into how cybersecurity awareness and training could be improved, including proposing a requirement that all seafarers undergo cybersecurity training and that it is undergone frequently. Awareness programs should include a real-life approach to cyber threats and best practices of cybersecurity in a way that is relatable and understandable for all involved parties. The overall security level can further be benefited by introducing a CySO, making cybersecurity training mandatory through the STCW, and ensuring that awareness and training measures are implemented at all levels of the organization.

As these are primarily suggestions, further research should be put into their effect and consequences. Making cybersecurity a requirement through regulatory means is not necessarily the right approach. This research does not reveal exactly what details should be put into an awareness program, what pedagogical tools should be used, or exactly how the training should be given. These are all topics suitable for future research.

The article has nevertheless given an insight into the current state of cybersecurity awareness of Turkish seafarers and proposed several ways to improve it. While this creates a basis for future research, it also gives valuable input to the maritime sector on what areas should be focused on to improve maritime cybersecurity awareness.

Appendix A: Appendix

The contents of the English version of the questionnaire used in this article are presented below.

Background Questions

In the following, you are presented with questions that have several alternatives. Please choose the answer that best fits your professional and educational background.

1. How long have you been working in the maritime sector?
   - Less than 1 year
   - Between 1 and 4 years
   - Between 5 and 15 years
   - More than 15 years
   - Never
2. What is your rank?
   - Master
   - Chief Officer
   - Officer on Watch (OOW)
   - Chief Engineer
   - Second engineer
   - Engineer Officer of the Watch (EOOW)
   - Electro Technical Officer (ETO)
   - Rating (Bosun / Fitter/ Oiler / Able Seaman / Ordinary Seaman / Cooker / Steward)
   - Deck cadet
   - Engine Cadet
   - Others
3. Which type of vessel did you work on in your last contract?
   - Dry cargo
   - Roll-on/roll-off (RORO)
   - Tanker
   - Passenger
   - Container
   - Others
   - I have never worked on a vessel
4. What is your highest level of education or training? Please check off ALL education you have completed in the list below. Example: Secondary school + Maritime High School + BSc (non-maritime)
   - Secondary school
   - Vocational training
   - High school (non-maritime)
   - Maritime High school
   - Vocational college (non-maritime)
   - Maritime college
   - BSc (non-maritime)
   - BSc (maritime)
   - MSc
   - PhD
5. Do you have formal education in information technology or cybersecurity?
   - No education
   - Short courses are taken in private
   - Short courses taken through the workplace
   - Formal education from college/university
   - Other
6. In your opinion, how good is your understanding of computers?
   - Very good
   - Good
   - Average
   - Poor
   - Very poor
7. In your opinion, who should be responsible for the cybersecurity of a vessel?
   - No one
   - Master
   - One of the other senior crew (C/E or C/O or 2/E)
   - Everyone onboard
   - Nominated staff at the office
8. How do you receive cybersecurity training in the workplace? Please choose ALL training forms you have in your workplace from the list below.
   - Onboard
   - At the shore
   - In-person
   - Remote (studying by yourself)
   - Online training
   - Other
   - I never received training in the workplace
9. How would you prefer to receive cybersecurity training?
   - I do not need cybersecurity training
   - In-person training
   - Online training
   - Remote (studying by yourself)
   - A combination of self-study, in-person and online training

10. How often do you receive cybersecurity training?
    - Never
    - Less than every five-year
    - Every five year
    - Once every two years
    - Once every year
    - More often than once every year
11. Has your company received remarks about cybersecurity after audits or inspections in the last 12 months? Please choose ALL of the remarks you have received in this period in the list below.
    - No
    - Yes, in SIRE
    - Yes, in CDI (Chemical Distribution Institute)
    - Yes, in port state
    - Yes, in flag state
    - Yes, in RightShip
    - Yes, in class society
    - Yes, in other

Personal Perception of Cybersecurity Topics

In the following you are presented with questions that have only two answer alternatives: Yes and No. Please choose the answer that best fits your opinion.

12. Has the cybersecurity training you attended included ship-specific attacks such as GPS jamming, AIS spoofing attacks or similar?
13. I am aware of cyber threats in my daily work
14. I know of a physical security breach within a vessel in my company within the last 12 months (ISPS Code violation)
15. I know of a cybersecurity breach within a vessel in my company within the last 12 months
16. Do you think cybersecurity training should be mandatory for all seafarers as per STCW?
17. In your opinion, do you think it is necessary to limit what websites are allowed to visit through the vessel wifi?
18. I believe that there is a need for additional training in cybersecurity in my workplace
19. I believe that senior crew (Master, chief engineer, chief officer, and 2nd Engineer) onboard a vessel consider cybersecurity important for the safety of the vessel
20. Does your company have guidelines for updating vessel navigation systems (e.g. Transfer systems, ECDIS, RADAR etc.) regularly?
21. Are computer systems (software, operating systems and antivirus) onboard your vessel updated regularly?

Scenario Questions

In the following you are presented with scenarios. Imagine yourself in these scenarios and choose the answer that best reflects your reaction.

22. Someone at the port asks you for the password to the vessel's wifi. How do you respond?
    - You check if the person has a good reason for asking and then share the password.
    - You share the password without asking any questions.
    - You refuse to share the password and immediately notify your superior.
    - You refuse to share the password, but log into the person's device so that he or she can get access to the wifi anyway.
23. You receive an email that tells you the vessel's antivirus is outdated and tells you to update it by clicking the attachment. How should you react?
    - You follow the instructions in the email and click the attachment to install the update.
    - You get suspicious of the email and report it to the IT department.
    - You show the email to your supervisor and ask them to check the attachment for you.
    - You ignore the instructions of the email and delete it.
24. When logging into a computer you are asked to update the password because the old one has expired. What should you do?
    - You type in the old password again so that you don't have to remember a new password.
    - You ask a colleague what password they are using and use the same password as him/her.
    - You create a new password based on the old password you were using.
    - You create a new password that is completely different from the old one.
25. You receive an email from someone asking you for details about vessel security routines. How do you react?
    - You ignore the email and delete it.
    - You contact your supervisor and report the email to him/her.
    - You write an email explaining that you do not know, but that the person can contact someone else in the company.
    - You write an email and try to explain the maintenance routines as well as you can.
26. While walking into the vessel, you find a USB memory stick. What do you do?
    - You do not pick up the USB device and let it stay in the same place.
    - You pick up the device and plug it into a computer on the vessel to check what is inside.

- You pick up the device and plug it into a personal computer to check what is inside.
- You inform your supervisor about the USB device.

27. You are asked to change the password for the ECDIS, GPS, purifier or similar, how do you store the password?
    - You write it down on a piece of paper and attach it to the component.
    - You do not write it down, but try to remember it in your mind.
    - You write it down in a dedicated list that your vessel has for passwords.
    - You write it down electronically and store it on the computer.

Acknowledgements We would like to express our sincere gratitude to all participants who contributed to our survey.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital) This article has received funding from the Research Council of Norway through the Maritime Cyber Resilience project (MarCy, Project Number 295077). The content reflects only the authors' views, and neither the Research Council of Norway nor the project partners are responsible for any use that may be made of the information it contains.

Data availability Survey data can be shared upon request.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

1. Alcaide, J.I., Llave, R.G.: Critical infrastructures cybersecurity and the maritime sector. Transp. Res. Procedia **45**, 547–554 (2020). https://doi.org/10.1016/j.trpro.2020.03.058
2. Ali, N.A.R.A., Chebotareva, A.A., Chebotarev, V.E.: Cyber security in marine transport: opportunities and legal challenges. Pomorstvo **35**(2), 248–255 (2021). https://doi.org/10.31217/p.35.2.7
3. Asariotis, R., et al.: Review of Maritime Transport 2020 (2020). https://unctad.org/webflyer/review-maritime-transport-2020
4. Asariotis, R., et al.: Review of Maritime Transport 2021 (2021). https://unctad.org/webflyer/review-maritime-transport-2021
5. Avanesova, T.P., et al.: Analysis of cyber-security aspects both ashore and at sea. In: IOP Conference Series: Earth and Environmental Science, vol. 872(1), p. 012024 (2021). https://doi.org/10.1088/1755-1315/872/1/012024
6. Bhatti, J., Humphreys, T.E.: Covert control of surface vessels via counterfeit civil GPS signals. Navigat. J. Inst. Navigat. **64**(1), 51–66 (2017). https://doi.org/10.1002/navi.183
7. Biau, D.J., Jolles, B.M., Porcher, R.: P Value and the theory of hypothesis testing: an explanation for new researchers. Clin. Orthop. Relat. Res. **468**, 885–892 (2010). https://doi.org/10.1007/s11999-009-1164-4
8. BIMCO. Cyber Security Workbook for On Board Ship Use, 3rd edn. Witherby Seamanship International (2021). ISBN: 9781914992094
9. BIMCO. The Guidelines on Cyber Security Onboard Ships, version 4. Tech. rep. (2020). https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx
10. Bolat, P., Kayişoğlu, G.: Antecedents and consequences of cybersecurity awareness: a case study for Turkish maritime sector. J. ETA Mar. Sci. **7**, 344–360 (2019). https://doi.org/10.5505/jems.2019.85057
11. Boyes, H., Isbell, R.: Code of practice: cyber security for ships. Institution of Engineering and Technology (2017). ISBN: 9781785615771
12. Burgess, T.F.: A general introduction to the design of questionnaires for survey research (2001)
13. Center for cybersikkerhed. Cybertruslen mod hjœlpemidler til navigation [Cyber threat against navigational aids]. Tech. rep. Center for cybersikkerhed (Centre for Cyber Security) (2022). https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cybertruslen-mod-hjalpemidler-til-navigation.pdf
14. Corradini, I.: Building a Cybersecurity Culture in Organizations—How to Bridge the Gap Between People and Digital Technology. Springer, Berlin (2020). https://doi.org/10.1007/978-3-030-43999-6
15. Croteau, B.: Lessons learned from teaching a maritime industrial control systems cybersecurity course. In: 2023 IEEE 48th Conference on Local Computer Networks (LCN), pp. 48–55 (2023). https://doi.org/10.1109/LCN58197.2023.10223335
16. Da Veiga, A., Martin, N.: Information security culture: a comparative analysis of four assessments. In: Devos, J., de Haas, S. (eds.) 8th European Conference on IS Management and Evaluation (ECIME 2014) (2014)
17. Da Veiga, A.: An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. Inf. Comput. Secur. **26**, 584–612 (2018). https://doi.org/10.1108/ICS-08-2017-0056
18. EduMaritime. Cyber Security Awareness for Seafarers Training & Certification Online - VIRSEC. https://www.edumaritime.net/virsec/cyber-security-awareness-for-seafarers
19. Erstad, E., et al.: A human-centred design approach for the development and conducting of maritime cyber resilience training. WMU J. Marit. Aff. **22**, 241–266 (2023). https://doi.org/10.1007/s13437-023-00304-7
20. Erstad, E., Ostnes, R., Lund, M.S.: An operational approach to maritime cyber resilience. TransNav **15**, 27–34 (2021). https://doi.org/10.12716/1001.15.01.01
21. Farah, M.A.B., et al.: Cyber security in the maritime industry: a systematic survey of recent advances and future trends. Information (Switzerland) (2022). https://doi.org/10.3390/info13010022
22. Fruth, M., Teuteberg, F.: Digitization in maritime logistics–What is there and what is missing? Cogent Bus. Manag. (2017). https://doi.org/10.1080/23311975.2017.1411066

23. Hanzu-Pazara, R., Raicu, G., Zagan, R.: The impact of human behaviour on cyber security of the maritime systems. Adv. Eng. Forum **34**, 267–274 (2019)
24. Heering, D., Maennel, O.M., Venables, A.N.: Shortcomings in cybersecurity education for seafarers. In: Guedes Soares, C., Santos, T.A. (eds.) Developments in Maritime Technology and Engineering, pp. 49–61. CRC Press, London (2021). https://doi.org/10.1201/9781003216582-06
25. Hopcraft, R.: Developing maritime digital competencies. IEEE Commun. Stand. Mag. **5**, 12–18 (2021). https://doi.org/10.1109/MCOMSTD.101.2000073
26. Hopcraft, R., Martin, K.M.: Effective maritime cybersecurity regulation—the case for a cyber code. J. Indian Ocean Region **14**, 354–366 (2018). https://doi.org/10.1080/19480881.2018.1519056
27. IMO. Member states. https://www.imo.org/en/OurWork/ERO/Pages/MemberStates.aspx (visited on 01/05/2024)
28. IMO. Resolution MSC.428(98) Maritime cyber risk management in Safety Management Systems. London (2017)
29. International Chamber of Shipping and BIMCO. Seafarer Workforce Report, 2021 Edition. (July 2021). https://www.ics-shipping.org/publication/seafarer-workforce-report-2021-edition/
30. International Maritime Organization (IMO). Guidelines On Maritime Cyber Risk Management - MSC-FAL.1-Circ.3. (2017). https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx
31. International Maritime Organization (IMO). International Convention on Standards of Training, Certification and Watchkeeping (STCW), 2010 Manila Amendments (1978)
32. International Transport Workers' Federation. STCW—A guide for seafarers (2014)
33. Jensen, L.: Challenges in maritime cyber-resilience. Technol. Innov. Manag. Rev. **5**, 35–39 (2015)
34. Kanwal, K., et al.: Maritime cybersecurity: are onboard systems ready? (2022). https://doi.org/10.1080/03088839.2022.2124464. https://www.tandfonline.com/doi/full/10.1080/03088839.2022.2124464
35. Karabacak, B., Sogukpinar, I.: ISRAM: information security risk analysis method. Comput. Secur. **24**(2), 147–159 (2005)
36. Karahalios, H.: Appraisal of a Ship's Cybersecurity efficiency: the case of piracy. J. Transp. Secur. **13**, 179–201 (2020). https://doi.org/10.1007/s12198-020-00223-1
37. Karamperidis, S., Kapalidis, C., Watson, T.: Maritime cyber security: a global challenge tackled through distinct regional approaches. J. Mar. Sci. Eng. (2021). https://doi.org/10.3390/jmse9121323
38. Kessler, G.C., Craiger, P., Haass, J.C.: A taxonomy framework for maritime cybersecurity: a demonstration using the automatic identification system. TransNav. Int. J. Mar. Navigat. Saf. Sea Transp. **12**, 429–437 (2018). https://doi.org/10.12716/1001.12.03.01
39. Kuhn, K., Bicakci, S., Shaikh, S.A.: COVID-19 digitization in maritime: understanding cyber risks. WMU J. Marit. Aff. **20**, 193–214 (2021). https://doi.org/10.1007/s13437-021-00235-1
40. Lane, J.M., Pretes, M.: Maritime dependency and economic prosperity: why access to oceanic trade matters. Mar. Policy (2020). https://doi.org/10.1016/j.marpol.2020.104180
41. Larsen, M.H., Lund, M.S.: A maritime perspective on cyber risk perception: a systematic literature review. IEEE Access **9**, 144895–144905 (2021). https://doi.org/10.1109/ACCESS.2021.3122433
42. Lee, S.H.: Constructing effective questionnaires. In: Pershing, J.A. (ed.) Handbook of Human Performance Technology: Principles, Practices, and Potential, 3rd edn, pp. 760–779 (2006)
43. Leite Junior, W.C., et al.: A triggering mechanism for cyber-attacks in naval sensors and systems. Sensors **21**, 3195 (2021). https://doi.org/10.3390/s21093195
44. Lund, M.S., Hareide, O.S., Jøsok, Ø.: An attack on an integrated navigation system. Necesse **3**, 149–163 (2018). https://doi.org/10.21339/2464-353x.3.2.149
45. Martins, N., Da Veiga, A.: The value of using a validated information security culture instrument. In: Devos, J., de Haas, S. (eds.) 8th European Conference on IS Management and Evaluation (ECIME 2014), pp. 146–154 (2014). https://www.researchgate.net/publication/266672235_The_Value_of_Using_a_Validated_Information_Security_Culture_Instrument
46. McGillivary, P.: Why maritime cybersecurity is an ocean policy priority and how it can be addressed. Mar. Technol. Soc. J. **52**, 44–57 (2018)
47. Meland, P.H., et al.: A retrospective analysis of maritime cyber security incidents. TransNav **15**, 519–530 (2021). https://doi.org/10.12716/1001.15.03.04
48. Mraković, I., Vojinović, R.: Maritime cyber security analysis—How to reduce threats? Trans. Mar. Sci. **8**, 132–139 (2019). https://doi.org/10.7225/toms.v08.n01.013
49. Mraković, I., Vojinović, R.: Evaluation of Montenegrin seafarers' awareness of cyber security. Trans. Mar. Sci. **9**, 206–216 (2020). https://doi.org/10.7225/toms.v09n02.005
50. Nikolov, D.B.: Maritime cybersecurity education and training at Nikola Vaptsarov naval academy. Pedagogika-Pedagogy **95**(6), 48–55 (2023). https://doi.org/10.53656/ped2023-6s.05
51. NORMA Cyber. NORMA Cyber Annual Threat Assessment 2022. Tech. rep. (2022). https://www.normacyber.no/news/norma-annual-threat-assessment-2022
52. Okoli, C.: A guide to conducting a standalone systematic literature review. Commun. Assoc. Inf. Syst. **37**(43), 879–910 (2015)
53. Oruc, A.: Tanker industry is more ready against cyber threats. In: International Conference on Marine Engineering and Technology Oman 2019 (ICMET Oman) (2019). https://doi.org/10.24868/icmet.oman.2019.030
54. Oruc, A., Chowdhury, N., Gkioulos, V.: A modular cyber security training programme for the maritime domain. Int. J. Inf. Secur. **23**, 1477–1512 (2024). https://doi.org/10.1007/s10207-023-00799-4
55. Pavur, J., et al.: A tale of sea and sky on the security of maritime VSAT communications. In: 2020 IEEE Symposium on Security and Privacy (SP), pp. 1384–1400 (2020). https://doi.org/10.1109/SP40000.2020.00056
56. Penn State's Department of Statistics. 2.3—Tukey Test for Pairwise Mean Comparisons—STAT 502. https://online.stat.psu.edu/stat502_fa21/lesson/2/2.3
57. Penn State's Department of Statistics. 2.4—Other Pairwise Mean Comparison Methods—STAT502. https://online.stat.psu.edu/stat502_fa21/lesson/2/2.4
58. Pentsov, D.A., Christodoulou-Varotsi, I.: Maritime Work Law Fundamentals: Responsible Shipowners, Reliable Seafarers. Springer, Berlin (2008). https://doi.org/10.1007/978-3-540-72751-4
59. Progoulakis, I., Rohmeyer, P., Nikitakos, N.: Cyber physical systems security for maritime assets. J. Mar. Sci. Eng. (2021). https://doi.org/10.3390/jmse9121384
60. Reegård, K., Blackett, C., Katta, V.: The concept of cybersecurity culture. In: Beer, M., Zio, E. (eds.) Proceedings of the 29th European Safety and Reliability Conference (ESREL), pp. 4036–4043 (2019). ISBN: 978-981-11-2724-3. https://doi.org/10.3850/978-981-11-2724-3_0761-cd
61. Rumsey, D.J.: Statistics for Dummies, 2nd edn. Wiley, Hoboken (2011)
62. Sanchez-Gonzalez, P.L., et al.: Toward digitalization of maritime transport? Sensors (Switzerland) (2019). https://doi.org/10.3390/s19040926
63. Saris, W.E., Gallhofer, I.N.: Design, evaluation, and analysis of questionnaires for survey research. In: Design, Evaluation, and Analysis of Questionnaires for Survey Research, 2nd. Wiley (2014)

64. Senarak, C.: Cybersecurity knowledge and skills for port facility security officers of international seaports: perspectives of IT and security personnel. Asian J. Ship. Logist. **37**, 345–360 (2021). https://doi.org/10.1016/j.ajsl.2021.10.002
65. Senarak, C.: Port cybersecurity and threat: a structural model for prevention and policy development. Asian J. Ship. Logist. **37**, 20–36 (2021). https://doi.org/10.1016/j.ajsl.2020.05.001
66. Shapiro, L.R., et al.: Trojan horse risks in the maritime transportation systems sector. J. Transp. Secur. **11**, 65–83 (2018). https://doi.org/10.1007/s12198-018-0191-3
67. Stoynov, S., Nikolov, B.: Approach to ship's it and ot systems cybersecurity improvement. Pedagogika-Pedagogy (2021). https://doi.org/10.53656/ped21-7s.16appr
68. Sullivan, L.: Hypothesis Testing—Analysis of Variance (ANOVA). Tech. rep. https://sphweb.bumc.bu.edu/otlt/mph-modules/bs/bs704_hypothesistesting-anova/bs704_hypothesistesting-anova_print.html
69. Svilicic, B., et al.: A study on cyber security threats in a shipboard integrated navigational system. J. Mar. Sci. Eng. (2019). https://doi.org/10.3390/jmse7100364
70. Svilicic, B., et al.: Maritime cyber risk management: an experimental ship assessment. J. Navig. **72**, 1108–1120 (2019). https://doi.org/10.1017/S0373463318001157
71. Svilicic, B., et al.: Raising awareness on cyber security of ECDIS. TransNav **13**, 231–236 (2019). https://doi.org/10.12716/1001.13.01.24
72. Svilicic, B., et al.: Paperless ship navigation: cyber security weaknesses. J. Transp. Secur. **13**, 203–214 (2020). https://doi.org/10.1007/s12198-020-00222-2
73. Svilicic, B., et al.: Towards a cyber secure shipboard radar. J. Navig. **73**, 547–558 (2020). https://doi.org/10.1017/S0373463319000808
74. TalTech. Introduction to cyber security. https://ois2.taltech.ee/uusois/subject/VLL1480
75. The National Cybersecurity Agency of France. Best practices for cyber security on board ships (2017)
76. Wood, C.C., Banks, W.W.: Human error: an overlooked but significant information security problem. Comput. Secur. **12**, 51–60 (1993). https://doi.org/10.1016/0167-4048(93)90012-T
77. Yamane, T.: Statistics: An Introductory Analysis, 2nd edn. Harper & Row, New York (1973)