Article

Challenges in Maritime Cybersecurity Training and Compliance

Divine C. Chupkemi * and Konstantinos Mersinas *

Posted Date: 28 August 2024

doi: 10.20944/preprints202408.2060.v1

Keywords: maritime cybersecurity; security awareness training; compliance; behaviour change

Article

Challenges in Maritime Cybersecurity Training and Compliance

Divine C. Chupkemi [1,*] and Konstantinos Mersinas [2]

[1] Department of Information Security, Royal Holloway University of London
[2] Department of Information Security, Royal Holloway University of London; Konstantinos.Mersinas@rhul.ac.uk
* Correspondence: Divine.Chupkemi.2019@live.rhul.ac.uk

Abstract: The implementation of cybersecurity standards and directives in the maritime sector plays a crucial role in protecting critical maritime infrastructures from cyber threats. The level of protection depends heavily on humans. However, the effectiveness of cybersecurity training and compliance programs, an essential component of these standards, is often hindered by challenges related to the sector's environment, including the established technologies, practices, and norms. This paper aims to identify these challenges through a literature review and set the basis for more effective human risk minimisation, responses, and training. We identify 18 challenges and validate them with an online survey (N=205) capturing real-world perspectives from maritime-related stakeholders. Our findings contribute to enhancing the effectiveness of maritime cybersecurity training and compliance programs, ultimately strengthening the maritime cybersecurity posture.

Keywords: maritime cybersecurity; security awareness training; compliance; behaviour change

1. Introduction

The maritime industry presents unique challenges for cybersecurity training due to its inherent organisational complexity and extensive regulations. Issues such as inadequate training opportunities, reluctance to adopt new technologies, unreliable internet connections, and multilingualism impede the implementation of traditional approaches to cybersecurity training [1].

This study aims to identify the training and compliance challenges that hinder the effectiveness of maritime cybersecurity training. By examining existing research, identifying the most significant training challenges in the maritime sector, and validating these findings through a survey of 205 individuals from different job functions and geographical locations in the maritime industry, we pinpoint the key obstacles which impede the deployment of effective cybersecurity training programs by maritime companies. Findings can serve as a basis for future research to develop practical solutions that benefit not only cybersecurity training but also other maritime training.

This paper is organised as follows: Section II outlines the importance of maritime cybersecurity and the role of the International Maritime Organization (IMO) by highlighting the efforts of IMO to promote cybersecurity training and compliance in the maritime industry and emphasising the critical need for such measures. Section III outlines the research methodology. Section IV covers ethical considerations, while section V offers an overview of existing literature on maritime cybersecurity training and compliance, including the challenges discussed and their impact on security measures. Section VI presents the survey design, validation, and results. Section VII discusses the survey results in relation to existing literature. Section VIII presents future research directions and limitations. The paper concludes in Section IX.

 doi:10.20944/preprints202408.2060.v1

2. Background

2.1. The International Maritime Organization (IMO)

In recent years, the maritime industry has become increasingly dependent on digital technologies, making it more vulnerable to cyber threats [2]. According to a report by the IMO [3], the maritime industry is experiencing an increase in cyber attack, with incidents ranging from phishing emails to ransomware attacks. These attacks exploit vulnerabilities in the industry's digital infrastructure, including outdated software, weak passwords, and inadequate cybersecurity measures [2]. One example of such an attack is the NotPetya ransomware attack in 2017 that targeted the computer systems of the Danish shipping company Maersk, causing widespread disruption and financial losses estimated at $300 million.

To address these challenges, the industry, acting through the IMO, adopted a new resolution in January 2021, Resolution MSC.428(98) [4], which established a mandatory regulatory framework that requires stakeholders to ensure their existing safety management systems (SMS) adequately address cyber risks and cybersecurity for ships.

In an attempt to promote more widely acceptable best practices for managing cybersecurity in the maritime industry, a supplement to IMO Resolution MSC.428(98) was introduced. The IMO guidelines on the management of maritime cyber risks (MSC-FAL.1/Circ.3) [5]. These guidelines, through the referencing of additional guidance and standards, including BIMCO's Guidelines on Cyber Security Onboard Ships [6], ISO/IEC 27001 [7], and the NIST Framework [8], offer recommendations, functional elements, to help maritime companies more flexibly and effectively implement and manage cyber risks and cybersecurity within their security management systems (SMS).

Despite potential shortcomings in specific content or guidance on cybersecurity training for maritime companies [20] the IMO acknowledges the growing significance of maritime cybersecurity and has undertaken efforts to tackle this issue. The adoption of Resolution MSC.428(98) and its accompanying guidelines, which stress the importance of implementing several layers of protection, including cybersecurity training and compliance for both onboard and offshore personnel, underscores IMO's effort to promote the necessity of effective cybersecurity training in the maritime sector, and the need for further research, to reinforce these efforts.

2.2. Importance of Cybersecurity Training and Compliance in Maritime

To underscore why identifying these challenges is of significant relevance, it is necessary to examine a number of studies that highlight the value of cybersecurity training and compliance in the maritime industry — and what they think needs to be done.

In the study on maritime cybersecurity threats and their impact, Chen et al. [11] provided an analysis of maritime cybersecurity threats, emphasising the necessity of training and compliance programs to mitigate cyber risks, and underscoring a holistic approach to cybersecurity. Building upon this, Hernandez et al. [13] examined the effectiveness of cybersecurity training for seafarers, suggesting that interactive, scenario-based training can enhance their ability to identify and respond to cyber attacks, thus promoting responsible behaviour. Similarly, Fenech et al. [14] identified challenges in providing cybersecurity training to port facility personnel, advocating for a comprehensive and coordinated approach that involves continuous training to keep pace with evolving threats while recommending stakeholder involvement in developing training programs. Høiback and Stål [16] further reiterated the significance of crew training, including incident reporting and response protocols, to enhance the cybersecurity posture of maritime organisations. Adding to this discourse, Pinto et al. [1] analysed existing training and compliance programs, calling for coordinated efforts, standardised content, and continuous updates to effectively address cybersecurity challenges. Taipale et al. [10] integrated human factors into cybersecurity training programs, identifying the lack of such training as a major concern, and emphasising the importance of human elements in maritime cybersecurity. Furthermore, Park and Campoy [15] evaluated the effectiveness of maritime cybersecurity training, highlighting the necessity of periodic assessments

 doi:10.20944/preprints202408.2060.v1

and feedback to ensure continuous improvement and engagement. Finally, to address the industry's human-centric vulnerabilities, Mersinas and Chupkemi [12] proposed models from behavioural economics and psychology, advocating for a cybersecurity training programs which foster behaviour change, thus, moving beyond mere awareness.

Collectively, these studies demonstrate the multifaceted and significant role of cybersecurity training and compliance in reducing risks and enhancing the cybersecurity posture of maritime organisations.

3. Methodology

We conducted a literature review to identify studies on cybersecurity training and compliance in the maritime industry. Different databases and resources were used, namely, Google Scholar, IEEE Xplore, OpenReview.net, the ACM Digital Library, ScienceDirect, JSTOR, and SpringerLink. The objective was to identify and evaluate academic journals, conference papers, industry reports, and government publications related to challenges inhibiting the effectiveness of maritime cybersecurity training and compliance. When the search term (‘maritime’ AND (‘cybersecurity’ OR ‘cyber security’)) was used, Google Scholar returned over 32,100 results, while IEEE Xplore and the ACM Digital Library each showed 1,204 and 1,011 results respectively. To refine the search, additional keywords were used, namely ((‘maritime’ AND (‘cybersecurity’ OR ‘cyber security’) AND ‘challenges’), with the additional term searches ‘training’ and ‘seafarers’. This approach, along with variations like ('information security’ AND ‘challenges’ AND ‘maritime'), and ‘human factors’ or ‘human aspects’ resulted in a manageable set of 185 relevant papers. These papers were further filtered using terms like ‘compliance challenges’, and ‘training and compliance’, with 70 included in our analysis.

In addition to the literature review, an online survey was administered to 213 participants (with 205 valid responses) through a purposive sampling process, which comprised maritime industry stakeholders, including managers and crew members. The survey ran for six months, from August 13th, 2023, to January 30th, 2024, during which participants were asked to provide their experiences and opinions concerning maritime cybersecurity training and compliance, and to identify any significant challenges associated with training and compliance. The anonymous online survey was designed to collect primary data from maritime-related individuals, information on their training experiences, challenges faced, and their individual suggestions for improvement. The survey was distributed through three main channels – maritime industry associations, professional networks, and social media platforms.

The targeted research question is the following:

- What are the training and compliance challenges inhibiting the effectiveness of maritime cybersecurity training and compliance?

And the associated objectives are:

- Identify and review the literature on training and compliance challenges in maritime cybersecurity training;
- Validate identified challenges via real-world perspectives from maritime stakeholders.

4. Ethics

The empirical research approach has been approved by the Royal Holloway, University of London Research Ethics Committee. Ethical considerations were taken into account throughout the research process. Participants were informed about the purpose of the research, their voluntary participation, and the confidentiality and anonymity of their responses. Informed consent was obtained from all participants before they started the survey, and no direct personal identifiable information was requested. The data collected was securely stored and only used for the purpose of this research. No personally identifiable information is included in the datasets.

 doi:10.20944/preprints202408.2060.v1

5. Challenges Inhibiting the Effectiveness of Maritime Cybersecurity Training and Compliance

Maritime cybersecurity training and compliance have become increasingly important in recent years due to the growing threat of cyber attacks on maritime infrastructure and vessels [9]. We provide an overview of existing literature on this topic, highlighting significant training and compliance challenges hindering the effective delivery of cybersecurity training.

5.1. Lack of Adequate Training

One of the earliest studies on maritime cybersecurity training was conducted by Jayawardena and Senarathna [17]. They highlight the lack of adequate cybersecurity training and compliance among maritime personnel as a significant obstacle to effective maritime cybersecurity training and recommend the development of comprehensive training programs to address this issue. The study emphasised the need for training programs that cover both technical aspects of cybersecurity and human factors, such as social engineering awareness. In a more recent study by Jin et al. [18], the authors examine the current state of maritime cybersecurity training in China. They find that while some training programs exist, they are often limited in scope and fail to adequately address the evolving cyber threats faced by the maritime industry, with only a small percentage of personnel receiving regular training [19]. The study recommends the development of a comprehensive national cybersecurity training framework for the maritime sector.

5.2. Lack of Specific Training Guidance

Another facet of the maritime, hindering the effectiveness of training and compliance, is the lack of specific cybersecurity training guidance. A study by Troncoso et al. [20] analysed the impact of international regulations and guidelines on maritime cybersecurity training. The authors find that while regulations such as the IMO provide a framework for cybersecurity training, there is still a lack of specific guidance on training methods and content. A flip side of this challenge is the complexity of compliance. The maritime industry is subject to several international regulations and guidelines. Ensuring compliance with these regulations can be complex and challenging, especially when it comes to cybersecurity [33]. A study by Zhang et al. [21] identifies that several maritime organisations have trouble developing effective maritime cybersecurity training programs due to the complexity and absence of a thorough and universally accepted framework.

5.3. Evolving Nature of Cyber Threats

The constantly evolving nature of cyber threats is also known to hinder effective cybersecurity training and compliance in the maritime sector [22]. Cybercriminals are continuously developing new tactics to exploit vulnerabilities in maritime systems. This necessitates regular updates to training plans to stay ahead of threats and ensure the security of maritime operations. However, the need for such frequent updates requires significant time, effort, and resources, with the rapid pace of technological advancements in the maritime sector further complicating the task of keeping training programs aligned with the latest threats and vulnerabilities [23]. Wang et al. [22] and Zhang et al. [23] stress the importance of continuously updating training programs to address these rapidly evolving threats. Their study suggests that regular assessments and collaboration with cybersecurity experts can help identify emerging threats and ensure training content remains relevant. Additional research by Yildirim and Mackay [48] indicates that adopting a dynamic and flexible training approach, such as using scenario-based exercises, can significantly improve maritime cybersecurity resilience.

5.4. Constantly Changing Risk Environment

A related challenge to the evolving nature of cyber threats is the constantly changing risk environment. Hopcraft [24] points out the difficulty of providing the appropriate level of competence in such a dynamic context. There are several complexities specific to maritime operations that need to be considered, including the diverse backgrounds and experiences of seafarers, varying levels of digital integration on ships, preconceived notions of cyber risk management among crew members,

 doi:10.20944/preprints202408.2060.v1

and diverse prior technological experience. It is important to note that the maritime sector does not only encompass ships and their crews, but also ports, enterprise centers, agents, and other service providers, all of whom have their own personnel and perform different tasks. These individuals also play a vital role in maritime cybersecurity, and any competence training or digital skill development should take their contributions into account [24]. Studies by Balduzzi et al. [49] and Svilicic and Rudan [50] stress the importance of addressing cultural and operational diversity in maritime cybersecurity training to keep up with changing risk profiles.

5.5. Complexity of Autonomous Ship Systems

A fifth significant challenge to the effective deployment of training and compliance in the maritime sector is the complexity of autonomous ship systems. Fully autonomous ships consist of integrated systems that communicate and collaborate with each other, providing real-time data for decision-making [25]. This complexity poses challenges for training programs as operators and engineers need to understand the intricate workings of these systems and how vulnerabilities in one component can affect the entire ship's cybersecurity [25]. A study by Sánchez Peña et al. [25] identified several key technical skills required, including knowledge of network protocols, data encryption, threat detection, incident response, and vulnerability management. In addition to technical skills, training programs must also address the socio-organisational aspects of cybersecurity [26]. Moreover, Johansson et al. [51] emphasised the need for comprehensive, hands-on training that includes simulated exercises and real-time system analyses to ensure readiness for autonomous ship operations.

5.6. Bring Your Own Device (BYOD) and Internet of Things (IoT)

The presence of Bring Your Own Device (BYOD) and the Internet of Things (IoT) on ships, which has revolutionised the maritime industry by enhancing communication, efficiency, and operations, has also been found to significantly hinder effective training and compliance. In the maritime industry, employees and crew members frequently use their personal devices while IoT-enabled systems monitor and control critical ship operations [27]. However, this transformation has brought a variety of cybersecurity challenges, including an increased attack surface where the combination of BYOD and IoT has increased the attack surface, and insecure devices (devices with inadequate security measures such as proper software and firmware updates), making ships vulnerable to attacks from multiple entry points [28,29]. Cybercriminals can easily gain unauthorised access to ship systems and data through these devices because they increase the attack surface and introduce vulnerabilities, with crew members and personnel usually without sufficient cybersecurity training, leading to risky behaviour and unintentional actions [30].

5.7. Lack of Practical Training Opportunities

Another challenge as identified by researchers is the lack of practical training opportunities. An effective cybersecurity training program requires hands-on experience and practical training opportunities. However, the maritime industry often lacks the necessary infrastructure and resources to provide such training [31]. This lack of practical training opportunities hinders the development of practical skills and limits the effectiveness of cybersecurity training and compliance. A study by Kim et al. [32] emphasised the need for practical training opportunities in maritime cybersecurity. The study suggested that partnerships between maritime organisations and cybersecurity training providers can help address this challenge by providing access to realistic training environments and simulations.

5.8. New Skills, Third Party Service Providers

In the modern world of complex digital systems on ships, it is becoming increasingly common for ship crews to rely on external engineers to maintain and service these systems [34]. This is because the crew may need to learn new skills to effectively monitor and maintain these advanced systems.

 doi:10.20944/preprints202408.2060.v1

These external engineers must also possess a deep understanding of the unique complexities of a ship's operations to ensure safe maintenance and cybersecurity [34]. It is worth noting that the majority of vulnerabilities discovered on ships are actually introduced by third parties, whether through mistakes or inadequate security measures [34]. This means that both crew members and third-party service providers need to possess the necessary technical knowledge and skills to ensure the safety and security of the maritime sector. Unfortunately, many of these third parties are unable to afford the investment required to attain this level of expertise [34], thereby reducing the effectiveness of maritime cybersecurity training and compliance.

5.9. Operational Limitations

First, given the limitations most shipping companies have over their IT infrastructure, and hence cybersecurity practices [35], the idea of frequent training or reminders if implemented is likely to be constrained to sections they have control over. Additionally, shipping companies are known to operate a fleet of hundreds of ships [36], some owned by them, and some contracted for a specific duration. Accordingly, these shipping companies, who might already be struggling with security onboard vessels they own, will not be able to manage cybersecurity onboard contracted vessels [35], leading to a substantial reduction in training programs related to maritime cyber security.

5.10. IT and OT Boundaries

The convergence of IT (Information Technology) and OT (Operational Technology) in the maritime industry introduces new challenges in cybersecurity training. Traditionally, IT and OT have been treated separately when it comes to training needs [37]. However, with ships and port infrastructure becoming more integrated with IT systems, the potential for cyber attacks is changing. This makes it increasingly difficult to provide ongoing tailored training and reminders to address these new challenges [37]. Studies by Parra et al. [52] and Sultana et al. [53] highlighted the need for dual-skilled professionals capable of understanding both IT and OT environments to effectively manage cybersecurity risks. Additionally, the lifespan of OT systems on ships may span decades, while IT systems have a much shorter lifespan. This creates challenges in addressing infrastructure that may be out of date and difficult to patch [43].

5.11. Limited Availability

Training and continuous learning opportunities for seafarers are often limited due to the nature of their work. Port calls, or scheduled stops at ports where ships dock for loading or unloading cargo, refuelling, or maintenance, and which are intended to provide time for relaxation and socialising, are frequently shortened, leaving seafarers with limited opportunities for training [24]. In addition, the international nature of operations and technical limitations of vessels make regular or ongoing training and reminders difficult to implement, resulting in a significant decrease in the effectiveness of maritime cybersecurity training and compliance [24]. Additionally, Miwa et al. [54] and Cedergren and Petersen [55] discuss how limited downtime affects the ability to conduct effective cybersecurity training on ships, exacerbating the skill gap and exposure to cyber risks.

5.12. Internet Access

Internet access on ships is another challenge for maritime training. While internet access is necessary for cybersecurity training and the secure management of internet-connected appliances, it is often limited in terms of bandwidth and availability while at sea or in international ports [38]. This poses constraints on the delivery of online training and updates on cyber hygiene practices by maritime organisations. However, shipping giants are now turning to high-speed connectivity and Low Earth Orbit (LEO) internet services, such as Starlink [46]. An adoption that is expected to see more maritime companies expand cloud solutions and digitise vessel operations more seamlessly, providing a promising solution to the long-standing issue of limited internet access [38]. Research by

 doi:10.20944/preprints202408.2060.v1

Mavropoulos et al. [56] and Karanikola et al. [2021] supports the adoption of advanced satellite communication technologies to enhance training efficacy and operational safety.

5.13. Long Travelling Times

The long duration of voyages in the maritime industry also impacts the frequency and effectiveness of training. Seafarers can spend days to months onboard a ship, making it challenging to provide regular and up-to-date training content, especially if face-to-face training is required. Additionally, crew turnover and interactions with different ports further complicate the training aspects of cybersecurity in the maritime [45]. Studies by Papanikolaou et al. [58] and Papazoglou et al. [59] discussed how the transient nature of seafaring work culture necessitates more flexible and frequent training solutions to maintain high levels of cybersecurity awareness.

5.14. Familiarity and Trust

Crew members spend extensive periods together on ships, leading to a heightened level of familiarity and trust. According to Bullough [47], familiarity among seafarers fosters a supportive work environment, which significantly impacts their behaviour and decision-making processes onboard ships. This familiarity often leads to the sharing of personal login credentials, including usernames and passwords, as an act of camaraderie and convenience. Such practices pose significant cybersecurity risks, undermining the effectiveness of training and compliance programs. Choi, Ahmed, and Ghorbani [39] highlight that credential sharing significantly increases the probability of unauthorised access and potential cyber threats. This behaviour weakens the ability to trace and prevent security breaches, as the attackers' actions could be attributed to multiple individuals sharing the same credentials.

5.15. Maritime Culture and Cultural Backgrounds

The culture within the maritime industry can also impact cybersecurity efforts. Legacy systems, convenience over security, and high complexity have been identified as cultural attributes that may hinder behaviour change and compliance [40–42]. Language and communication barriers also pose challenges in maritime cybersecurity training. Ships are often operated by crew members from different nationalities who speak different languages. This can make it difficult to communicate expectations, risks, and priorities related to cybersecurity [38]. It can also affect the ability to communicate management support, which is crucial for cybersecurity training and compliance.

5.16. Ship Entertainment for Crew

Ship entertainment systems, including onboard entertainment platforms, Wi-Fi networks, and IPTV systems, can be potential entry points for cyber attackers. These systems often rely on outdated software and lack proper security measures, making them susceptible to exploitation [43]. Attacks on ship entertainment systems can enable adversaries to gain unauthorised access to critical ship systems. For instance, research demonstrates how vulnerabilities in ship entertainment systems can be exploited to control critical functions such as steering and engine systems [44]. This underscores the need for addressing ship entertainment as part of comprehensive cybersecurity training and compliance programs.

In conclusion, there are several challenges that maritime cybersecurity training and compliance face. These challenges still exist in the industry and have a significant impact on training crew members — ultimately hindering the effectiveness of maritime cybersecurity measures.

6. The Survey

The purpose of the online survey was to gather primary data from individuals working in the maritime industry. The survey aimed to collect information about their training and compliance experiences, the challenges they face, and their suggestions for improvement. The survey was anonymous and distributed through three main channels – industry associations (List of

 doi:10.20944/preprints202408.2060.v1

emails/contacts in the industry), professional networks (YouGov), and social media platforms (LinkedIn, WhatsApp Group, Facebook). The survey targeted maritime-related individuals in different roles and levels of responsibility, including seafarers, IT personnel, and management personnel.

6.1. Development of Survey Questions

When developing the survey questions, the aim was to gather comprehensive insights into the training and compliance challenges faced by the maritime personnels by making sure the questions covered a wide range of topics and designed to elicit specific and actionable responses from the participants.

The presented themes were informed by our identified challenges. An initial list of questions was then formed and closely reviewed to ensure the questions were clear, concise, and relevant to the objective.

Another aspect that was carefully considered was the anonymity and confidentiality of respondents, which included a disclaimer at the beginning of the survey, assuring participants that their responses would be kept confidential and used only for the purposes of analysis and improvement.

The survey includes questions related to familiarity with cybersecurity training, participation in such training, preferred training delivery methods, convenience of the current training method, and the biggest obstacles to taking cybersecurity training. The survey also explored the potential usefulness of an AI-based cybersecurity awareness trainer. By addressing these questions, the survey aimed to provide valuable insights that could help improve training and compliance practices in the maritime industry.[1]

6.2. Justification for Survey Format and Questionnaire Structure

An online survey format was chosen for several reasons. Firstly, it provided an easy reach to the targeted participants from different geographical locations, ensuring a diverse range of perspectives and experiences. Secondly, it allowed participants to respond to the survey at their own pace and at a convenient time.

The questionnaire structure was designed to have a thematic coherence and flow smoothly. Starting with demographic questions to gather information about the participants' age, roles, and experience levels. Next, we asked participants targeted questions about training programs and their effectiveness, compliance challenges, and improvement suggestions. A combination of multiple-choice questions, rating scales, and open-ended questions were used to gather both quantitative and qualitative data.

6.3. Survey Results

Once the survey responses were collected, descriptive statistics were employed to analyse and identify trends, patterns, and correlations within the data. The survey was administered to 213 participants (with 205 valid responses) from various professional positions in maritime and geographical locations. The participants were randomly selected to ensure representation. Out of the valid responses, 69.7% were male, 25.7% were female, and 4.6% preferred not to disclose their sex. Among their job titles 18% were officers, masters, captains, watch leaders, and medical pursers, 10.2% engineers, 5.1% stewards, 4% mates, 3% cooks, and the remainder did not specify or were retired.

When asked about their familiarity with cybersecurity training, 57% stated that they are familiar with cybersecurity training, while 41% said they are unsure, and 2% are not fully aware of what it entails.

---

[1] A copy of the survey can be found at: qfreeaccountssjc1.az1.qualtrics.com

Note: we will provide a permanent link, if needed.

 doi:10.20944/preprints202408.2060.v1

When asked if they had ever taken part in any cybersecurity training offered by their company, 39% responded positively, while 61% responded negatively. Among those who had taken part in such training, 81% were unable to specify the type of training method used from the following options: lecture-based training in a classroom or conference hall, web-based training, or self-training accessible online, remotely, through a third party, or from the relevant department. 11.3% reported that the training was web-based self-training that could be accessed online, 5% reported it was lecture-based training, while 1% said it was delivered remotely by a third party or the responsible department.

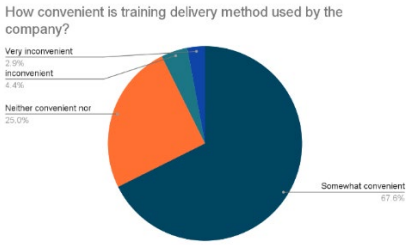

Figure 1. How convenient is the training delivery method used by the company?

In terms of convenience, 67.6% respondents found the training delivery method used by their company to be somewhat convenient, 25% said it was neither convenient nor inconvenient, 4.4% found it inconvenient, 2.9% found it very inconvenient, and the rest were uncertain.

Participants were also asked about the most useful methods of training delivery. Out of the options presented, 5.3% selected lecture-based classroom/conference hall training delivered at the head-office, 8% chose lecture-based classroom/conference hall training delivered on-deck, 41.3% preferred web-based self-training accessible online from any device, 24% selected web-based self-training, 17.3% choose an option not listed, and 4% opted for remotely delivered by a third-party expert or the department in charge.

Finally, participants were asked an open statement about the biggest obstacle to undergoing cybersecurity training as an employee in the maritime industry. While 45.8% of respondents were unsure, the rest mentioned factors such as lack of time, cost, difficulty in finding a safe space to complete the training, lack of interest, job obligations, being at sea during training on land, time management, lack of impact visibility, limited device access, workload, organisational challenges, and poor training quality. Direct expressions included statements such as “The time to fit in the training with obligations of the job”, “Lack of time and motivation”, “Safe space to complete the training”, “It's not interesting enough so people don't engage”, “Age and understanding”, “People rarely see the impact so don't see the training as required.”, “Understanding the been benefits”, “People feel that they have more important issues to worry about”, “Takes up time”, “It is a fast changing industry”, “Being informed about the cybersecurity available”, “Getting the time to complete the training”, “Being busy all the time, but I think it is very helpful”.

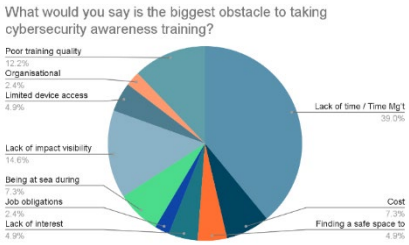

Figure 2. What would you say is the biggest obstacle to taking cybersecurity training?

 doi:10.20944/preprints202408.2060.v1

6.4. Findings

We identified and interpreted the following key training and compliance challenges from the survey responses. Firstly, a significant challenge highlighted by participants is the lack of knowledge and familiarity with cybersecurity training. Many respondents expressed uncertainty regarding this topic, indicating a gap and potential risk. Secondly, participants expressed a desire for more thorough and customised training programs, indicating that current training programs were too generic and did not sufficiently cover the specific compliance needs of their roles and departments. They requested more hands-on and role-specific training to improve their comprehension and implementation of compliance principles. This is supported by the fact that 14% of respondents mentioned a "lack of impact visibility", whereas 12% mentioned “poor training quality” as the main obstacles to undergoing cybersecurity training as maritime industry employees.

The survey provided valuable insights into the challenges faced in deploying an effective maritime cybersecurity training program. The following are five key observations based on the survey results:

6.4.1. Lack of Awareness

The survey highlights that a significant number of participants are either unsure or not fully aware of what cybersecurity training entails. This lack of understanding indicates a lack of maturity and a need for better communication and education regarding the importance and benefits of cybersecurity training in the maritime industry. It is likely that both the individual’s skillsets and the environment contribute to this phenomenon.

6.4.2. Low Participation Rate

The survey indicates that the majority of participants have not taken part in any cybersecurity training offered by their company. This is concerning as it might suggest that organisations are struggling to engage employees and encourage their active participation.

6.4.3. Unclear Training Delivery Methods

Another important finding is that many participants who had undergone cybersecurity training were unable to specify the type of training delivery methods used. This indicates a lack of clarity and consistency in the way training programs are structured and communicated to employees, resulting in confusion and lack of understanding amongst program recipients.

6.4.4. Convenience of Training

The survey reveals mixed responses regarding the convenience of the training programs. While a significant number of participants found the training delivery method somewhat convenient, a considerable number were unsure or found it inconvenient. This might suggest that usability and accessibility aspects of training programs are not being currently considered.

6.4.5. Obstacles to Training

The survey captures obstacles that hinder employees from undergoing cybersecurity training. Factors such as lack of time, cost, and limited device access were reported as the most common barriers.

7. Summary of Key Findings and Challenges

Our investigation uncovers significant deficiencies in both cybersecurity training and compliance among maritime personnel, emphasising the urgent necessity for comprehensive training programs that not only address technical aspects but also consider human factors.

Compounding these challenges are evolving cyber threats, the complexities of autonomous systems, the prevalence of Bring Your Own Device (BYOD) and Internet of Things (IoT) technologies

 doi:10.20944/preprints202408.2060.v1

on ships, and various compliance issues. Language barriers, crew trust dynamics, and cultural tendencies that prioritise convenience over security further intensify these concerns. The table below summarises the key challenges identified and validated through the survey, complete with detailed descriptions.

Table 1. Summary of key findings.

Challenge	Description
1. Lack of awareness and familiarity with cybersecurity	Seafarers and maritime-related personnel have limited knowledge of cybersecurity best practices and are unaware of potential consequences.
2. Constantly evolving nature of cyber threats, insufficient training scope.	Cyber threats are constantly changing and evolving, requiring regular updates to training programs. Existing training programs in the maritime industry are often limited in scope and fail to adequately address evolving cyber threats.
3. Risk environment complexities	The maritime sector has complexities, such as diverse backgrounds and experiences of seafarers, varying levels of digital integration on ships, preconceived notions of cyber risk management, and diverse prior technological experience.
4. Complexity of autonomous ship systems	Autonomous systems introduce new challenges for training as operators and engineers must grasp intricate interdependencies and vulnerabilities within integrated systems while also developing essential technical and socio-organisational skills for effective cybersecurity management.
5. IT and OT boundaries	The increasing integration of IT and OT systems necessitates the development of dual-skilled professionals who can navigate the complexities of both environments while addressing the vulnerabilities of ageing infrastructure prone to cyber attacks.
6. Bring Your Own Device (BYOD) and Internet of Things (IoT) challenges	The use of personal devices and IoT-enabled systems on ships increases the attack surface and introduces potential vulnerabilities. Lack of awareness and insecure devices pose challenges.
7. Limited availability of training opportunities	Seafarers often have limited time for training due to the nature of their work and long travelling times.
8. Language and communication barriers	Crew members from different nationalities and language backgrounds may face challenges in understanding cybersecurity expectations.
9. Familiarity and trust risks	High levels of familiarity and trust among crew members can lead to risky behaviour, such as sharing login credentials.
10. Organisational culture and legacy systems	Organisational culture, legacy systems, convenience over security, and high complexity can hinder behaviour change and compliance.
11. Ship entertainment system vulnerabilities	Ship entertainment systems can serve as potential entry points for cyber attackers, and their outdated software and lack of security measures make them susceptible to exploitation.
12. Limited internet access	Limited bandwidth and availability of internet access at sea or in international ports pose constraints on the delivery of online training and updates.

 doi:10.20944/preprints202408.2060.v1

13. Compliance challenges	Compliance with national and international regulations and guidelines can be challenging, with difficulties in interpretation and implementation, which can vary significantly across different regions.
14. Unfavourable conditions for behaviour change interventions	The presence of obstacles such as limited time, lack of interest, job commitments, distance from training locations, and poor training quality makes it even more challenging to practically implement effective behaviour change interventions.
15. Absence of specific guidance on training methods and content	While the International Maritime Organization offers a flexible framework for cybersecurity training that acknowledges diverse operational environments, the lack of specific guidance on training methods and content may result in inconsistent quality, necessitating specialised solutions for effective and standardised training.
16. Financial constraints	Financial constraints and the complexity and cost of implementing effective cybersecurity training programs can be challenges for maritime organisations.
17. Low participation rates	The survey results show a lack of knowledge and familiarity with cybersecurity training and low participation rates in training programs.
18. The need for thorough and customised training programs	Survey participants expressed a desire for more thorough and customised training programs that are role-specific and provide hands-on experience.

8. Future Research Directions and Limitations

8.1. Future Research Directions

Challenges identified in this study were discussed based on their impact and prevalence within the maritime sector, offering a clearer roadmap for future interventions and improvements. To remedy these challenges, it is vital to implement improved communication strategies, innovative awareness initiatives, incentive programs, and flexible training options, all of which are essential for strengthening maritime cybersecurity and protecting the industry against emerging threats. Our conclusions present several areas where future research can focus for improving maritime cybersecurity training and compliance.

One area of interest is the development of advanced training programs that address both the technical aspects of cybersecurity and the human factors involved, with an intention of changing individuals' behaviours. It is important to create standardised frameworks and guidelines that align with international regulations and guidelines, but which are customised to people's roles, skillsets, and needs.

Another important area of research is the utilisation of machine learning and artificial intelligence towards enhancing cybersecurity training and compliance. This area overlaps with the previous one to shift the traditional approaches to training and awareness into new personalised and dynamic directions.

8.2. Limitations

Despite the insights and findings provided by this study, several limitations must be acknowledged that could influence the overall results and the applicability of our conclusions.

The survey utilised a purposive sampling method to gather input from, primarily maritime industry stakeholders, including managers and crew members. While this approach aimed to target those most familiar with cybersecurity practices, it may have resulted in a sample that lacks diversity in terms of roles and geographical representation within the maritime industry. The perspectives of

 doi:10.20944/preprints202408.2060.v1

less represented roles, such as IT specialists or security officers, were not specifically included, which may lead to an incomplete understanding of the challenges present across the entire sector.

Then, the survey responses are self-reported data regarding participants' experiences and opinions on cybersecurity training and challenges. Such data can be subject to bias, including social desirability bias, where respondents may provide answers they believe are expected or acceptable, rather than their genuine views. This limitation could skew the results, leading to an overestimation or underestimation of issues concerning training effectiveness, familiarity with cybersecurity, and participation rates.

Finally, the research was conducted over a limited timeframe, with the survey running from August 2023 to January 2024. Although this period provided a snapshot of current perceptions and challenges, it might be limiting in comparison to continuous longitudinal studies. Cybersecurity is an evolving field, and insights drawn from continuous trends over time can be more insightful.

9. Conclusions

In this paper we present the challenges and insights gathered from existing literature and a survey which paint a vivid picture of the current state of maritime cybersecurity training. The literature establishes a foundational understanding of common challenges and trends, while our survey results bring forth firsthand perspectives from maritime industry professionals. Notably, both the challenges outlined, and the survey results highlight a significant gap in awareness among maritime personnel regarding the critical importance of cybersecurity training.

For instance, the survey revealed that many participants are either unsure or lack a complete understanding of what cybersecurity training involves. This lack of clarity may stem from a variety of factors, such as the fast-paced nature of maritime operations or the overwhelming volume of regulations maritime personnel must navigate, as outlined in the challenges identified. In addition, challenges identified underscore the concerning trend of low participation rates in cybersecurity training programs, particularly among smaller maritime organisations. This observation is strikingly supported by the survey, where a majority of respondents indicated they had not engaged in any cybersecurity training offered by their employers.

Another critical area of exploration was the convenience of training. While the challenges identified highlighted the necessity for accessible and usable training programs tailored to the maritime industry, the survey revealed mixed responses regarding their actual convenience. This disparity might indicate a disconnect between the availability of such programs and their practical implementation within daily operations.

Moreover, the challenges identified 18 obstacles that impede effective cybersecurity training, ranging from limited resources to the complexities associated with rolling out comprehensive training programs. Echoing these challenges, survey participants pointed out barriers like lack of time and funds, as well as limited access to necessary devices for effective training. Such findings suggest that while there is a recognition of the need for training, practical considerations often hinder participation.

Appendix A

Maritime CyberSecurity Awareness Survey

References

1. Pinto, A.; Roldan, P.; Wind, P. A.; Argudo, E. Analysis of training and awareness programs on maritime cybersecurity. In Proceedings of the 2017 International Conference on Cyber Security and Protection of Digital Services, 2017.
2. Akpan, F.; Bendiab, G.; Shiaeles, S.; Karamperidis, S.; Michaloliakos, M. Cybersecurity Challenges in the Maritime Sector. Network 2022, 2(1), 123–138. https://doi.org/10.3390/network2010009.
3. International Maritime Organization (IMO). Cyber Security in the Maritime Sector: A Review of Current Threats and Measures Taken by the IMO and Stakeholders. 2019. Available online: https://www.imo.org/en/OurWork/Security/SecurityPolicies/Pages/Cyber-Security.aspx.

4. International Maritime Organization (IMO). Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. 2017.
5. International Maritime Organization (IMO). MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management. 2017.
6. BIMCO et al. Guidelines on Cyber Security Onboard Ships, Version 4; BIMCO: Copenhagen, Denmark, 2021. Available online: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships (accessed on 16 October 2021).
7. ISO/IEC. Information Technology — Security Techniques — Information Security Management Systems — Requirements. ISO/IEC 27001:2013. Available online: https://www.iso.org/standard/54534.html.
8. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. 2014. Available online: https://www.nist.gov/cyberframework.
9. Maritime Safety Committee. Enhancing Maritime Cybersecurity: Policies and Practices. International Maritime Organization, 2022. Available online: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx (accessed on 14 November 2023).
10. Taipale, K.; Grönman, J.; Lyra, M. Human Factors Affecting Maritime Cybersecurity: A Systematic Review. Journal of Maritime Research 2018, 15(1), 21–40.
11. Chen, Z.; Liu, P.; Lee, S. Analysis and Evaluation of Maritime Cybersecurity Threats and Their Impacts. Maritime Policy & Management 2020, 47(5), 682–698. https://doi.org/10.1080/03088839.2020.1744520.
12. Mersinas, K.; Chupkemi, D. C. Reducing the Cyber-Attack Surface in the Maritime Sector via Individual Behaviour Change. In Proceedings of the CYBER 2022 - The Seventh International Conference on Cyber-Technologies and Cyber-Systems: CYMAR - Cyber at Sea; 2022.
13. Hernandez, F.; Lee, J.; Park, S. Cybersecurity Awareness Training for Seafarers. Journal of Maritime Research 2021, 18(3), 245–263.
14. Fenech, F.; Davidsson, P.; Ekstedt, M. Cybersecurity Training for Port Facility Personnel. Transportation Research Part C: Emerging Technologies 2018, 93, 246–262.
15. Park, S.; Campoy, L. Assessing the Effectiveness of Maritime Cybersecurity Training Programs. Journal of Maritime Studies 2019, 46(3), 345–360.
16. Høiback, E.; Stål, L. Maritime Cybersecurity Incidents and Training. Journal of Maritime Research 2020, 17(1), 39–52.
17. Jayawardena, S. A. D. K.; Senarathna, S. M. A. W. Maritime Cyber Security Training and Compliance - An Overview. International Journal of Computer Applications 2016, 133(11). https://doi.org/10.5120/ijca2016909486.
18. Jin, L.; Zhang, Y.; Ma, L.; Zhang, D. Maritime Cybersecurity Training and Awareness in China: A Critical Review. Journal of Maritime Policy & Management 2020, 47(3), 343–361.
19. Cho, J.; Nguyen, T. T.; Jin, D. W.; Jang, J. Y.; Kim, C. S. A Study on Cyber Security Awareness and Training Needs of Maritime Organization. International Journal of Innovative Technology and Exploring Engineering 2018, 7(7), 1081–1086.
20. Troncoso, A. J. C.; Min, G.; Song, D. Cybersecurity Training in the Maritime Sector: A Review. Journal of Marine Science and Engineering 2019, 7(10), 323. https://doi.org/10.3390/jmse7100323.
21. Zhang, J.; Shou, Y.; Li, X. Cybersecurity Awareness Enhancement Toward Employees in Maritime Organisations. Journal of Marine Science and Engineering 2020, 8(4), 287. https://doi.org/10.3390/jmse8040287.
22. Wang, Y. L.; Stringhini, G.; Egele, M.; Vanbever, L.; Holz, R. Fear and Hacking in Las Vegas: Lessons from DEFCON-27's Capture the Flag Competition. arXiv preprint arXiv:2003.00267.
23. Zhang, J.; Liu, Z.; Lou, W.; Orosz, G. Cybersecurity Education and Training: Connecting Research, Practice, and Policy. Computers & Security 2020, 97, 101962.
24. Hopcraft, M. Managing Maritime Cyber Risks: Complexity, Competency, and Crew. Journal of Maritime Law and Commerce 2020, 51(1), 25–44.
25. Sánchez Peña, R.; Amaya, J.; García, J.; Fuentes, L.; Abella, A.; Devos, A. Identifying Skills for Cybersecurity in Autonomous Ships. In Proceedings of the 2020 7th International Symposium on Digital Forensic and Security (ISDFS); IEEE, 2020; pp. 1–5.
26. Matusiak, M.; Ferreira, R.; Onori, M.; Petit, J. Cybersecurity Challenges in Autonomous Ships: A Survey. Journal of Marine Science and Engineering 2020, 8(6), 443.
27. Cheng, W.; Yang, C.; Ghorbani, A. IoT Device Classification and Attribute Identification through Deep Learning. Proceedings of the 33rd Annual ACM Symposium on Applied Computing 2018, 300–305. https://doi.org/10.1145/3167132.3167391.
28. Khan, Y. M.; Bhaskaran, S. Challenges in the Internet of Things for Maritime Cybersecurity. Procedia Computer Science 2019, 159, 950–955. https://doi.org/10.1016/j.procs.2019.09.176.
29. Douligeris, C.; Mitrou, L. Internet of Things (IoT): Security Challenges, Privacy Issues, and Proposed Solutions. Computer Communications 2016, 32(12), 977–987. https://doi.org/10.1016/j.comnet.2016.02.016.

30. Gebhardt, S.; Koppenhoefer, S.; Thiele, L. Towards Cybersecurity Awareness in Crew-Centric Ship Operation. Journal of Navigation 2017, 70(1), 87–104. https://doi.org/10.1017/S0373463316000483.
31. Awad, M.; Elaziz, M. Factors Affecting Maritime Cybersecurity Awareness and Education: A Case from Egypt. Journal of Transportation Security 2019, 12(4), 99–112.
32. Kim, S. J.; Park, S.; Lee, J. Enhancing Maritime Cybersecurity Readiness: Focusing on Training and Human Factors. IEEE Access 2019, 7, 23433–23441.
33. Menzel, J.; Frias-Martinez, E.; Foufou, S.; Theodorakopoulos, G. Interdependencies in Maritime Cybersecurity: A Game-Theoretic Analysis. IEEE Journal on Selected Areas in Communications 2019, 37(5), 1131–1146.
34. Tierney, A. HackTheSea, Speed 2 – The Poseidon Adventure. Available online: https://www.pentestpartners.com/security-blog/speed-2-the-poseidon-adventure-when-cruise-ships-attack-part-1/ (accessed 12 December 2022).
35. Jensen, L. Challenges in Maritime Cyber-Resilience. Technology Innovation Management Review 2015, 5(4), 35–39.
36. Shipping Fleet Statistics 2021. GOV.UK. Available online: https://www.gov.uk/government/statistics/shipping-fleet-statistics-2021/shipping-fleet-statistics-2021--2 (accessed 13 January 2023).
37. Tam, K.; Jones, K. Factors Affecting Cyber Risk in Maritime. In Proceedings of the 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA); pp. 1–8. https://doi.org/10.1109/CyberSA.2019.8899382.
38. Erstad, E.; Hopcraft, R.; Vineetha Harish, A.; et al. A Human-Centred Design Approach for the Development and Conducting of Maritime Cyber Resilience Training. WMU Journal of Maritime Affairs 2023. https://doi.org/10.1007/s13437-023-00304-7.
39. Choi, Y.; Ahmed, R.; Ghorbani, A. A. Seaside: A Multi-Modal Approach for Building Awareness in Maritime Cybersecurity. Computers in Human Behavior 2018, 81, 324–335.
40. Martins, E. F.; Eloff, J. H. P. Information Security Culture in the Maritime Industry. Computers & Security 2002, 21(6), 570–578.
41. Dennis, S.; Gradwell, P.; Jefferies, N.; Perkins, C. Maritime Cyber Security: Identifying Cultural Inhibitors to Behaviour Change and Compliance. In Proceedings of the 2018 International Conference on Cyber Security and Internet of Things (CSIT); pp. 99–104.
42. Da Veiga, A.; Eloff, J. H. P. The Nature of Maritime Cyber Security. In Maritime Safety, Security and Piracy; Perez, C., Ed.; Springer: 2010; pp. 89–106.
43. Bothur, D.; Zheng, G.; Valli, C. A Critical Analysis of Security Vulnerabilities and Countermeasures in a Smart Ship System. In Proceedings of the 15th Australian Information Security Management Conference; Edith Cowan University: Perth, Western Australia, 2017; pp. 81–87.
44. Cheng, J.; Xing, X.; Li, Z.; Li, P.; Yang, X. Vulnerability Analysis of Passenger Ships Based on the Shipboard Entertainment System. Ocean Engineering 2020, 215, 108169.
45. Tam, K.; Jones, K. Maritime Cybersecurity Policy: The Scope and Impact of Evolving Technology on International Shipping. Journal of Cyber Policy 2018, 3(1). https://doi.org/10.1080/23738871.2018.1444384.
46. Mitsui O.S.K. Lines, Ltd.; Marlink AS. Revolutionizing Maritime Connectivity: Leveraging the LEO Satellite Networks for Enhanced Connectivity. 2023. Available online: https://safety4sea.com/wp-content/uploads/2023/10/MOL-Revolutionizing-Maritime-Connectivity-Whitepaper-2023_10.pdf.
47. Bullough, A. (2019). Trust at sea. In A paradigm shift: Creating sustainable maritime futures (pp. 89-104). Springer.
48. Yildirim, E.; Mackay, M. Scenario-Based Training in Maritime Cybersecurity. Journal of Maritime Technology and Innovation 2021, 15(2), 101–115.
49. Balduzzi, M.; Pasta, A.; Wilhoit, K. A Security Evaluation of AIS Automated Identification System. In Proceedings of the 30th Annual Computer Security Applications Conference; 2014; pp. 436–445.
50. Svilicic, B.; Rudan, I. Cybersecurity Challenges in Maritime Operations: Cultural and Operational Considerations. International Journal of Maritime Technology 2019, 29(3), 64–78.
51. Johansson, P.; Luengo-Oroz, M. A.; Penttinen, P. Complexity of Autonomous Systems and Cybersecurity Training. Journal of Autonomous Maritime Ecosystems 2016, 13(1), 22–35.
52. Parra, F.; Mercade, J.; Villa, C. Integrating IT and OT in Maritime Systems for Enhanced Cybersecurity. International Journal of Maritime Cyber-Infrastructure 2019, 47(2), 123–137.
53. Sultana, S.; Rahman, M.; Tiwari, P. Securing the Convergence of IT and OT in Maritime. Maritime Digitalization Review 2020, 25(3), 78–97.
54. Miwa, T.; Tsukuo, K.; Saito, Y. Impact of Limited Downtime on Cybersecurity Training in Maritime. Seafarers' Cybersecurity Practices 2019, 33(2), 99–110.
55. Cedergren, A.; Petersen, K. Challenges in Maritime Cybersecurity: Limited Training Opportunities. Harbors and Ports Review 2017, 19(4), 45–61.

 doi:10.20944/preprints202408.2060.v1

56. Mavropoulos, Y.; Malakasiotis, E.; Drosos, S. Adopting Advanced Satellite Communication for Maritime Training. Journal of Maritime Communications Technology 2019, 40(3), 150–167.
57. Karanikola, L.; Tsigkou, A.; De Nys, H. Enhancing Cybersecurity Training with High-Speed Connectivity. Maritime Cyber Technology Journal 2021, 32(1), 12–25.
58. Papanikolaou, A.; Tsoukalas, N.; Vakkas, G. Influence of Long Voyages on Cybersecurity Training. International Journal of Maritime Safety and Wellness 2018, 45(2), 88–102.
59. Papazoglou, E. P.; Ganas, I. A.; Koutoumanos, A. Flexible Training Solutions for Maritime Cybersecurity. Global Maritime Training Review 2020, 27(1), 55–69.