Journal of
Marine Science and Engineering

IMPACT FACTOR 2.7

CITESCORE 4.4

Article

Challenges in Maritime Cybersecurity Training and Compliance

Divine C. Chupkemi and Konstantinos Mersinas

Special Issue
Advanced Research in Shipping Informatics and Communications—2nd Edition

Edited by
Prof. Dr. Nikitas Nikitakos and Dr. Iosif Progoulakis

MDPI

https://doi.org/10.3390/jmse12101844

Journal of
Marine Science and Engineering

MDPI

Article

Challenges in Maritime Cybersecurity Training and Compliance

Divine C. Chupkemi * and Konstantinos Mersinas *

Department of Information Security, Royal Holloway University of London, Egham TW20 0EX, UK
* Correspondence: divine.chupkemi.2019@live.rhul.ac.uk (D.C.C.); konstantinos.mersinas@rhul.ac.uk (K.M.)

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 programmes, 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 minimization, responses, and training. We identify 17 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 programmes, ultimately strengthening the maritime cybersecurity posture.

Keywords: maritime cybersecurity; cybersecurity training; training challenges; compliance challenges

Citation: Chupkemi, D.C.; Mersinas, K. Challenges in Maritime Cybersecurity Training and Compliance. *J. Mar. Sci. Eng.* **2024**, *12*, 1844. https://doi.org/10.3390/jmse12101844

Academic Editors: Nikitas Nikitakos and Iosif Progoulakis

Received: 27 August 2024
Revised: 26 September 2024
Accepted: 4 October 2024
Published: 15 October 2024

1. Introduction

The maritime industry presents unique challenges for cybersecurity training due to its inherent organizational 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]. Effective cybersecurity training in this context is further complicated by diverse crew compositions, varied levels of digital literacy, and inherently dynamic operational environments [2]. Vessels often operate in geographically isolated regions [3], whilst the maritime workforce regularly transitions between onshore and offshore environments, notwithstanding the high turnover rate of crew members, which necessitates frequent training sessions [4], complicating the delivery of consistent and standardized cybersecurity training. These factors create a complex backdrop against which training programmes must be developed and implemented, requiring a tailored approach that takes into account the unique constraints and needs of the maritime sector.

This study aims to identify the training and compliance challenges that hinder the effectiveness of maritime cybersecurity training and compliance. 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 programmes 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 organized as follows: Section 2 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 emphasizing the critical need for such measures. Section 3 outlines the research methodology. Section 4 covers ethical considerations, while Section 5 offers an overview of existing literature on maritime cybersecurity training and compliance, including the challenges discussed and their impact on security measures. Section 6

presents the survey design, validation, and results. Section 7 discusses the survey results in relation to the existing literature, including future research directions and limitations. The paper concludes in Section 8.

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 [5]. According to a report by the IMO [6], the maritime industry is experiencing an increase in cyber attacks, 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 [5]. One example of such an attack is the NotPetya ransomware attack in 2017, which primarily targeted Ukraine's M.E.Doc accounting software but significantly affected the Danish shipping company Maersk as collateral damage, causing widespread disruption and financial losses estimated at EUR 300 million. The attack forced Maersk to reinstall its entire IT infrastructure, affecting operations across 130 countries and causing severe delays in global shipping and logistics.

To address these challenges, the industry, acting through the IMO, adopted a new resolution in January 2021, Resolution MSC.428(98) [7], 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 practises 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) [8]. These guidelines, through the referencing of additional guidance and standards, including BIMCO's Guidelines on Cyber Security Onboard Ships [9], ISO/IEC 27001 [10], and the NIST Framework [11], offer recommendations and functional elements, to help maritime companies more flexibly and effectively implement and manage cyber risks and cybersecurity within their security management systems (SMSs).

Despite potential shortcomings in specific content or guidance on cybersecurity training for maritime companies, 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 the 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 achieved.

In the study on maritime cybersecurity threats and their impact, Chen et al. [12] provided an analysis of maritime cybersecurity threats, emphasizing the necessity of training and compliance programmes 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 behavior. 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 programmes. Høiback and Stål [15] further reiterated the significance of crew training, including incident reporting and response protocols, to enhance the cybersecurity posture of maritime organizations. Adding to this

discourse, Pinto et al. [1] analyzed existing training and compliance programmes, calling for coordinated efforts, standardized content, and continuous updates to effectively address cybersecurity challenges. Taipale et al. [16] integrated human factors into cybersecurity training programmes, identifying the lack of such training as a major concern and emphasizing the importance of human elements in maritime cybersecurity. Furthermore, Park and Campoy [17] evaluated the effectiveness of maritime cybersecurity training, highlighting the necessity of periodic assessments and feedback to ensure continuous improvement and engagement. Finally, to address the industry's human-centric vulnerabilities, Mersinas and Chupkemi [18] proposed models from behavioral economics and psychology, advocating for cybersecurity training programs which foster behavior 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 organizations.

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 returned 1204 and 1011 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 in relation to 'compliance challenges' and 'training and compliance', resulting in 70 being included in our analysis.

The inclusion criteria encompassed peer-reviewed articles, industry reports, conference papers, and government publications within the timeframe of 2010 to 2023, focused on English-language sources, and the searches were conducted between February 2021 and November 2023 by a team of two researchers, to strengthen the reliability and validity of the process. Among the exclusion criteria are papers not focused on the maritime sector, opinion pieces, editorial comments, and redundant studies.

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 13 November 2023 to 30 April 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?

The associated objectives are as follows:

- Identify and review the literature on training and compliance challenges in maritime cybersecurity training;

- Validate identified challenges via real-world perspectives from maritime stakeholders.
- A copy of the survey results is included in Supplementary Materials.

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 personally identifiable information was requested. The data collected were securely stored and only used for the purpose of this research. No personally identifiable information is included in the datasets.

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 [19]. We provide an overview of the 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 in 2016 [20]. 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 programmes to address this issue. The study emphasizes the need for continuous educational interventions as part of training frameworks to combat the lack of adequate understanding among maritime personnel. In a more recent study by Jin et al. [21], the authors examine the current state of maritime cybersecurity training in China. They find that while some training programmes exist, most of them lack the sufficient scope and fail to adequately address cyber threats faced by the maritime industry, with only a small percentage of personnel receiving regular training [22]. 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 sector hindering the effectiveness of training and compliance is the lack of specific cybersecurity training guidance. A study by Troncoso et al. [23] analyzed 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. A study by Zhang et al. [24] identified that several maritime organizations have trouble developing effective maritime cybersecurity training programmes 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 [25]. 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 programmes aligned with the latest threats and vulnerabilities [26]. Wang et al. [25] and Zhang et al. [26] stress the importance of continuously updating training programmes 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 [27] 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 [28] 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, and diverse prior technological experience. It is important to note that the maritime sector not only encompasses ships and their crews but also ports, enterprise centres, 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 [28]. Studies by Balduzzi et al. [29] and Svilicic and Rudan [2] 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 [30]. This complexity poses challenges for training programmes 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 [30]. A study by Sánchez Peña et al. [30] 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 programmes must also address the socio-organizational aspects of cybersecurity [31]. Moreover, Johansson et al. [32] emphasized 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 revolutionized the maritime industry by enhancing communication, efficiency, and operations, has also been found to significantly hinder effective training and compliance. It is important to note that general awareness of BYOD and IoT-related risks is essential; however, the focus here is on formal training programmes and compliance measures that address these specific challenges. In the maritime industry, employees and crew members frequently use their personal devices while IoT-enabled systems monitor and control critical ship operations [33]. However, this transformation has brought a variety of cybersecurity training and compliance 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 [34,35].

Cybercriminals can easily gain unauthorized 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 behavior and unintentional actions [36].

5.7. Lack of Practical Training Opportunities

Another challenge, as identified by researchers, is the lack of practical training opportunities. An effective cybersecurity training programme requires hands-on experience and practical training opportunities. However, the maritime industry often lacks the necessary infrastructure and resources to provide such training [37]. 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. [38] emphasized the need for practical training opportunities in maritime cybersecurity. The study suggested that partnerships between maritime organizations 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 [39]. This is because the crew may need to learn new skills to effectively monitor and maintain these advanced systems. These external engineers must also possess a deep understanding of the unique complexities of a ship's operations to ensure safe maintenance and cybersecurity [39]. It is worth noting that the majority of vulnerabilities discovered on ships are introduced by third parties, whether through mistakes or inadequate security measures [39]. 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 [39], 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 practises [40], 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 [41], 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 [40], leading to a substantial reduction in training programmes related to maritime cybersecurity.

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 [42]. 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 [42]. Studies by Parra et al. [43] and Sultana et al. [44] 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.

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, of which are intended to provide time for relaxation and socializing, are frequently shortened, leaving seafarers with limited opportunities for training [28]. 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 [28]. Additionally, Miwa et al. [45] and Cedergren and Petersen [46] discuss how limited downtime affects the ability to conduct effective cybersecurity training on ships, exacerbating the skills gap and exposure to cyber risks.

5.12. 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 [4,47]. Attacks on ship entertainment systems can enable adversaries to gain unauthorized 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 [48]. This underscores the need for addressing ship entertainment as part of comprehensive cybersecurity training and compliance programmes.

5.13. Familiarity and Trust

Crew members spend extensive periods together on ships, leading to a heightened level of familiarity and trust. According to Bullough [49], familiarity among seafarers fosters a supportive work environment, which significantly impacts their behavior 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 practises pose significant cybersecurity risks, undermining the effectiveness of training and compliance programmes. Choi, Ahmed, and Ghorbani [50] highlight that credential sharing significantly increases the probability of unauthorized access and potential cyber threats. This behavior weakens the ability to trace and prevent security breaches, as the attackers' actions could be attributed to multiple individuals sharing the same credentials.

5.14. 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 [3]. This poses constraints on the delivery of online training and updates on cyber hygiene practises by maritime organizations. However, shipping giants are now turning to high-speed connectivity and Low Earth Orbit (LEO) internet services, such as Starlink [51]. An adoption that is expected to see more maritime companies expand cloud solutions and digitize vessel operations more seamlessly, providing a promising solution to the long-standing issue of limited internet access [3]. Research by Mavropoulos et al. [52] and Karanikola et al. [53] supports the adoption of advanced satellite communication technologies to enhance training efficacy and operational safety.

5.15. Long Travelling Times

The long duration of voyages in the maritime industry also impacts the frequency and effectiveness of cybersecurity 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 [4]. Studies

by Papanikolaou et al. [54] and Papazoglou et al. [55] discuss how the transient nature of seafaring work culture necessitates more flexible and frequent training solutions to maintain high levels of cybersecurity competence.

5.16. 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 behavior change and compliance [56,57]. 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. It can also affect the ability to communicate management support, which is crucial for cybersecurity training and compliance.

5.17. Security Fatigue

A remaining challenge is mitigating security fatigue among maritime personnel, a concept where the over-saturation of security protocols can lead to negligence or disengagement [58]. In the context of the maritime industry, seafarers and other maritime personnel are often required to adhere to numerous cybersecurity practises amidst their regular duties, which can lead to a sense of being overwhelmed. This constant exposure can result in decreased vigilance, compliance, and overall interest in maintaining high cybersecurity standards. Over time, crew members may become less attentive to security requirements, start ignoring alerts, or fail to follow protocols consistently, which can increase the risk of cyber incidents. To combat this, innovative methods such as game-based training may be explored. Game-based solutions provide a practical, engaging way to simulate real-world cyber threats, helping seafarers develop skills and effectively respond to incidents without the associated risks [59]. Such methods make training more appealing and relevant, addressing long-standing critiques about traditional training programmes' lack of engagement and effectiveness.

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 emails/contacts in the industry), professional networks (YouGov), and social media platforms (LinkedIn, WhatsApp groups, 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 personnel by making sure the questions covered a wide range of topics and were 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' data, 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 trainer. By addressing these questions, the survey aimed to provide valuable insights that could help improve training and compliance practises in the maritime industry (A copy of the survey questions can be found at qfreeaccountssjc1.az1.qualtrics.com (accessed on 4 March 2023). Note: we will provide a permanent link if needed).

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 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 programmes 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

We employed descriptive statistics on the collected data. The survey was administered to 213 participants (with 205 valid responses) from various professional positions in maritime and geographical locations. Participants were randomly selected to ensure representation.

We acknowledge that there may be a sampling bias as participation was voluntary and uncontrolled. Eight invalid responses were excluded due to incomplete data. The survey was pre-tested with a small pilot group, and questions were reviewed for clarity to mitigate language barriers and increase response accuracy and reliability.

Out of the valid responses, 69.7% were male, 25.7% 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.

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.

In terms of convenience, as depicted in Figure 1 below, 67.6% of 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.

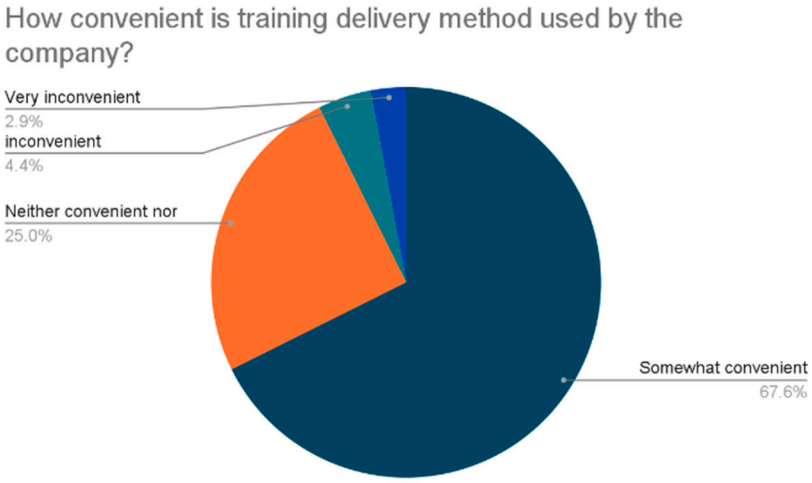

Figure 1. How convenient is the training delivery method used by the company?

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 to provide input 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, organizational 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", and "Being busy all the time, but I think it is very helpful".

6.4. Findings

As depicted in Figure 2, we identify and interpret 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 customized training programmes, indicating that current training programmes 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 obstacle for undergoing cybersecurity training as maritime industry employees.

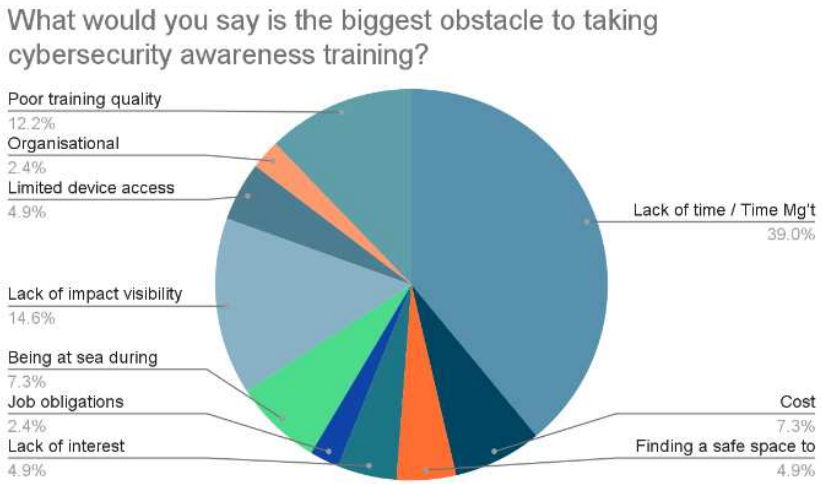

Figure 2. What would you say is the biggest obstacle to taking cybersecurity training?

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

6.4.1. Lack of Value Perception

The survey highlights that a significant number of participants are either unsure or not fully aware of what cybersecurity training entails. This lack of value perception indicates 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 skillset 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 organizations 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 programmes are structured and communicated to employees, resulting in confusion and lack of understanding amongst programme recipients.

6.4.4. Convenience of Training

The survey reveals mixed responses regarding the convenience of the training programmes. 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 programmes are not currently being 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. Discussion and Future Research Directions

The survey findings underscore significant gaps and challenges in the realm of maritime cybersecurity training and compliance, reflecting broader trends identified in the

existing literature. Consistently, both our data and the literature emphasize the importance of comprehensive and contextualized training programmes. Studies like those by Chen et al. [12] and Fenech et al. [14] underline the necessity of integrating both technical skill development and human factors awareness to achieve effective cybersecurity training and compliance postures. For example, Fenech et al. advocate for continuous training that evolves with emerging cyber threats, a recommendation echoed by Wang et al. [25] and our survey participants, who expressed a strong need for ongoing, relevant, and practical training, especially given the rapidly changing threat landscape in maritime operations.

However, an emergent inconsistency between our survey results and some literature highlights the complexity and varied perceptions within the industry. While Park and Campoy [17] emphasize periodic assessments and feedback for maintaining training engagement, our survey reveales mixed responses about the convenience and practical usability of existing training programmes. This disparity points to an urgent need for more flexible, adaptable training solutions that accommodate the diverse schedules and operational environments of maritime personnel. Addressing this gap may involve leveraging emerging technologies, such as virtual reality (VR) and augmented reality (AR), to provide immersive, scenario-based training modules that can be accessed remotely and during off-peak operational periods.

7.1. Future Research Directions

Moving forward, research should prioritize several key areas to enhance the efficacy of maritime cybersecurity training and compliance. First, there is a pressing need to develop and deploy advanced communication strategies within maritime organizations. These strategies must aim to raise awareness about the critical importance of cybersecurity training and effectively articulate its benefits. Enhanced communication can mitigate gaps in understanding and foster a culture of cybersecurity awareness and responsibility at all organizational levels.

Further, future research should explore the implementation of incentive-based training programmes. Introducing incentives for active participation in cybersecurity training can significantly improve engagement rates. Such incentives might include certifications, monetary rewards, or career advancement opportunities linked to demonstrated cybersecurity competencies. Moreover, the study of innovative training methodologies, particularly those grounded in gamification and experiential learning, could yield valuable insights. Game-based training, for instance, has shown promise in mitigating security fatigue by offering a more engaging and less monotonous training experience [59].

Lastly, the dynamic nature of cyber threats necessitates continuous adaptation and evolution of training programmes. Research should focus on the integration of artificial intelligence (AI) and machine learning (ML) to personalize training content dynamically, ensuring relevance and immediacy. AI-driven analytics can identify patterns in user behavior and tailor training modules to individual needs, thereby enhancing retention and application of cybersecurity principles. Additionally, the development of standardized yet customizable frameworks, grounded in international regulatory standards but adaptable to various maritime roles and operational contexts, can help streamline training efforts and ensure consistency across the industry.

7.2. Limitations

Despite the insights and findings provided by this study, several limitations must be acknowledged. The survey utilized a purposive sampling method targeting maritime industry stakeholders, including managers and crew members, which may have resulted in a sample lacking diversity in terms of roles and geographical representation. Perspectives from less represented roles, such as IT specialists or security officers, were not specifically included, leading to a potentially incomplete understanding of challenges across the sector.

Additionally, the survey relied on self-reported data, which can be subject to biases like social desirability bias. This can skew results, leading to an overestimation or underestimation of issues related to training effectiveness and participation rates.

Finally, the research was conducted over a limited timeframe, from August 2023 to January 2024. Although providing a snapshot of current perceptions and challenges, this period might be limiting compared to continuous longitudinal studies. Cybersecurity is an evolving field; hence, insights drawn from continuous trends over time can be more enlightening.

8. Conclusions

In this paper, we presented the challenges and insights gathered from existing literature and a survey, painting 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 survey results highlight a significant gap in training and compliance among maritime personnel regarding the critical importance of cybersecurity training.

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 factors such as the fast-paced nature of maritime operations or the overwhelming volume of regulations maritime personnel must navigate. Additionally, the challenges identified underscore a concerning trend in low participation rates in cybersecurity training programmes, particularly among smaller maritime organizations. This observation is supported by the survey, where many 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 the necessity for accessible and usable training programmes 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 programmes and their practical implementation within daily operations.

Moreover, the challenges identified include obstacles like limited resources and the complexities associated with rolling out comprehensive training programmes. 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. These findings emphasize the need to delineate between general awareness issues and specific challenges relating to the deployment and effectiveness of cybersecurity training and compliance programmes. Practical considerations, including time, cost, and access constraints, often hinder participation, suggesting a targeted approach to training and compliance solutions is necessary.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/jmse12101844/s1. Maritime CyberSecurity Awareness Survey.

Author Contributions: Conceptualization, K.M. and D.C.C.; methodology, D.C.C.; validation, K.M.; formal analysis, D.C.C.; investigation, K.M. and D.C.C.; resources, K.M.; data curation, D.C.C.; writing—original draft preparation, D.C.C.; writing—review and editing, K.M.; visualization, D.C.C.; supervision, K.M.; project administration, K.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data supporting the reported results can be found in Supplementary Materials.

Conflicts of Interest: The authors declare no conflict of interest.

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, London, UK, 19–20 June 2017.
2. Svilicic, B.; Rudan, I. Cybersecurity Challenges in Maritime Operations: Cultural and Operational Considerations. *Int. J. Marit. Technol.* **2019**, *29*, 64–78.
3. 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), Oxford, UK, 3–4 June 2019; pp. 1–8. [CrossRef]
4. Cheng, J.; Xing, X.; Li, Z.; Li, P.; Yang, X. Vulnerability Analysis of Passenger Ships Based on the Shipboard Entertainment System. *Ocean Eng.* **2020**, *215*, 108169.
5. Akpan, F.; Bendiab, G.; Shiaeles, S.; Karamperidis, S.; Michaloliakos, M. Cybersecurity Challenges in the Maritime Sector. *Network* **2022**, *2*, 123–138. [CrossRef]
6. 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 (accessed on 12 September 2021).
7. International Maritime Organization (IMO). *Resolution MSC.428(98)—Maritime Cyber Risk Management in Safety Management Systems*; IMO: London, UK, 2017.
8. International Maritime Organization (IMO). *MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management*; IMO: London, UK, 2017.
9. BIMCO; OCIMF; INTERTANKO; International Chamber of Shipping; IUMI; WSC. *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).
10. *ISO/IEC 27001*; Information Technology—Security Techniques—Information Security Management Systems—Requirements. Available online: https://www.iso.org/standard/54534.html (accessed on 16 October 2021).
11. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. 2014. Available online: https://www.nist.gov/cyberframework (accessed on 16 October 2021).
12. Chen, Z.; Liu, P.; Lee, S. Analysis and Evaluation of Maritime Cybersecurity Threats and Their Impacts. *Marit. Policy Manag.* **2020**, *47*, 682–698. [CrossRef]
13. Hernandez, F.; Lee, J.; Park, S. Cybersecurity Awareness Training for Seafarers. *J. Marit. Res.* **2021**, *18*, 245–263.
14. Fenech, F.; Davidsson, P.; Ekstedt, M. Cybersecurity Training for Port Facility Personnel. *Transp. Res. Part C Emerg. Technol.* **2018**, *93*, 246–262.
15. Høiback, E.; Stål, L. Maritime Cybersecurity Incidents and Training. *J. Marit. Res.* **2020**, *17*, 39–52.
16. Taipale, K.; Grönman, J.; Lyra, M. Human Factors Affecting Maritime Cybersecurity: A Systematic Review. *J. Marit. Res.* **2018**, *15*, 21–40.
17. Park, S.; Campoy, L. Assessing the Effectiveness of Maritime Cybersecurity Training Programs. *J. Marit. Stud.* **2019**, *46*, 345–360.
18. 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, Valencia, Spain, 13–17 November 2022.
19. 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).
20. Jayawardena, S.A.D.K.; Senarathna, S.M.A.W. Maritime Cyber Security Training and Compliance—An Overview. *Int. J. Comput. Appl.* **2016**, *140*. [CrossRef]
21. Jin, L.; Zhang, Y.; Ma, L.; Zhang, D. Maritime Cybersecurity Training and Awareness in China: A Critical Review. *J. Marit. Policy Manag.* **2020**, *47*, 343–361.
22. 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. *Int. J. Innov. Technol. Explor. Eng.* **2018**, *7*, 1081–1086.
23. Troncoso, A.J.C.; Min, G.; Song, D. Cybersecurity Training in the Maritime Sector: A Review. *J. Mar. Sci. Eng.* **2019**, *7*, 323. [CrossRef]
24. Zhang, J.; Shou, Y.; Li, X. Cybersecurity Awareness Enhancement Toward Employees in Maritime Organisations. *J. Mar. Sci. Eng.* **2020**, *8*, 287. [CrossRef]
25. 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* **2020**, arXiv:2003.00267.
26. Zhang, J.; Liu, Z.; Lou, W.; Orosz, G. Cybersecurity Education and Training: Connecting Research, Practice, and Policy. *Comput. Secur.* **2020**, *97*, 101962.
27. Yildirim, E.; Mackay, M. Scenario-Based Training in Maritime Cybersecurity. *J. Marit. Technol. Innov.* **2021**, *15*, 101–115.
28. Hopcraft, M. Managing Maritime Cyber Risks: Complexity, Competency, and Crew. *J. Marit. Law Commer.* **2020**, *51*, 25–44.
29. Balduzzi, M.; Pasta, A.; Wilhoit, K. A Security Evaluation of AIS: Automated Identification System. In Proceedings of the 30th Annual Computer Security Applications Conference, New Orleans, LA, USA, 8–12 December 2014; pp. 436–445.
30. 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), San Antonio, TX, USA, 29–30 April 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–5.

31. Matusiak, M.; Ferreira, R.; Onori, M.; Petit, J. Cybersecurity Challenges in Autonomous Ships: A Survey. *J. Mar. Sci. Eng.* **2020**, *8*, 443.
32. Johansson, P.; Luengo-Oroz, M.A.; Penttinen, P. Complexity of Autonomous Systems and Cybersecurity Training. *J. Auton. Marit. Ecosyst.* **2016**, *13*, 22–35.
33. Cheng, W.; Yang, C.; Ghorbani, A. IoT Device Classification and Attribute Identification through Deep Learning. In Proceedings of the 33rd Annual ACM Symposium on Applied Computing, Pau, France, 9–13 April 2018; pp. 300–305. [CrossRef]
34. Khan, Y.M.; Bhaskaran, S. Challenges in the Internet of Things for Maritime Cybersecurity. *Procedia Comput. Sci.* **2019**, *159*, 950–955. [CrossRef]
35. Douligeris, C.; Mitrou, L. Internet of Things (IoT): Security Challenges, Privacy Issues, and Proposed Solutions. *Comput. Commun.* **2016**, *32*, 977–987. [CrossRef]
36. Gebhardt, S.; Koppenhoefer, S.; Thiele, L. Towards Cybersecurity Awareness in Crew-Centric Ship Operation. *J. Navig.* **2017**, *70*, 87–104. [CrossRef]
37. Awad, M.; Elaziz, M. Factors Affecting Maritime Cybersecurity Awareness and Education: A Case from Egypt. *J. Transp. Secur.* **2019**, *12*, 99–112.
38. Kim, S.J.; Park, S.; Lee, J. Enhancing Maritime Cybersecurity Readiness: Focusing on Training and Human Factors. *IEEE Access* **2019**, *7*, 23433–23441.
39. 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 on 12 December 2022).
40. Jensen, L. Challenges in Maritime Cyber-Resilience. *Technol. Innov. Manag. Rev.* **2015**, *5*, 35–39. [CrossRef]
41. Shipping Fleet Statistics 2021. GOV.UK. Available online: https://www.gov.uk/government/statistics/shipping-fleet-statistics-2021/shipping-fleet-statistics-2021--2 (accessed on 13 January 2023).
42. Erstad, E.; Hopcraft, R.; Vineetha Harish, A.; Tam, K. A Human-Centred Design Approach for the Development and Conducting of Maritime Cyber Resilience Training. *WMU J. Marit. Aff.* **2023**, *22*, 241–266. [CrossRef]
43. Parra, F.; Mercade, J.; Villa, C. Integrating IT and OT in Maritime Systems for Enhanced Cybersecurity. *Int. J. Marit. Cyber-Infrastruct.* **2019**, *47*, 123–137.
44. Sultana, S.; Rahman, M.; Tiwari, P. Securing the Convergence of IT and OT in Maritime. *Marit. Digit. Rev.* **2020**, *25*, 78–97.
45. Miwa, T.; Tsukuo, K.; Saito, Y. Impact of Limited Downtime on Cybersecurity Training in Maritime. *Seafar. Cybersecur. Pract.* **2019**, *33*, 99–110.
46. Cedergren, A.; Petersen, K. Challenges in Maritime Cybersecurity: Limited Training Opportunities. *Harb. Ports Rev.* **2017**, *19*, 45–61.
47. 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, Perth, Australia, 5–6 December 2017; pp. 81–87.
48. Tam, K.; Jones, K. Maritime Cybersecurity Policy: The Scope and Impact of Evolving Technology on International Shipping. *J. Cyber Policy* **2018**, *3*, 147–164. [CrossRef]
49. Bullough, A. Trust at Sea. In *A Paradigm Shift: Creating Sustainable Maritime Futures*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 89–104.
50. Choi, Y.; Ahmed, R.; Ghorbani, A.A. Seaside: A Multi-Modal Approach for Building Awareness in Maritime Cybersecurity. *Comput. Hum. Behav.* **2018**, *81*, 324–335.
51. Mitsui, O.S.K.; Lines, Ltd.; Marlink, A.S. 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 (accessed on 14 November 2023).
52. Mavropoulos, Y.; Malakasiotis, E.; Drosos, S. Adopting Advanced Satellite Communication for Maritime Training. *J. Marit. Commun. Technol.* **2019**, *40*, 150–167.
53. Karanikola, L.; Tsigkou, A.; De Nys, H. Enhancing Cybersecurity Training with High-Speed Connectivity. *Marit. Cyber Technol. J.* **2021**, *32*, 12–25.
54. Papanikolaou, A.; Tsoukalas, N.; Vakkas, G. Influence of Long Voyages on Cybersecurity Training. *Int. J. Marit. Saf. Wellness* **2018**, *45*, 88–102.
55. Papazoglou, E.P.; Ganas, I.A.; Koutoumanos, A. Flexible Training Solutions for Maritime Cybersecurity. *Glob. Marit. Train. Rev.* **2020**, *27*, 55–69.
56. Martins, E.F.; Eloff, J.H.P. Information Security Culture in the Maritime Industry. *Comput. Secur.* **2002**, *21*, 570–578.
57. Dennis, S.; Gradwell, P.; Jefferies, N.; Perkins, C. Maritime Cyber Security: Identifying Cultural Inhibitors to Behaviour Change and Compliance. In Proceedings of the International Conference on Cyber Security and Internet of Things (CSIT), Amman, Jordan, 11–12 July 2018; pp. 99–104.
58. Stanton, B.; Theofanos, M.F.; Prettyman, S.S.; Furman, S. Security Fatigue. *IT Prof.* **2016**, *18*, 26–32. [CrossRef]
59. Menzel, J.; Frias-Martinez, E.; Foufou, S.; Theodorakopoulos, G. Interdependencies in Maritime Cybersecurity: A Game-Theoretic Analysis. *IEEE J. Sel. Areas Commun.* **2019**, *37*, 1131–1146.