International Journal of Information Security
https://doi.org/10.1007/s10207-023-00799-4

REGULAR CONTRIBUTION

A modular cyber security training programme for the maritime domain

Aybars Oruc[1] · **Nabin Chowdhury**[1] · **Vasileios Gkioulos**[1]

Abstract
The global maritime industry is continuing the rapid digitization of systems and dependency on advancing technology, in a trend akin to other industrial domains. One of the main issues that this integration has brought is an increased vulnerability to a growing number of cyber threats. While several security measures are being implemented to prevent or respond to cyber attacks, the human element is still one of the main weaknesses. Many of today's cyber attacks take advantage of human personnel's lack of awareness, which makes cyber security awareness and training activities of critical importance. Unfortunately, current research is still limited in its offerings for cyber security training specific to maritime personnel. Moreover, such training programmes for the professionals should be developed role-based in accordance with the suggestions of many credited maritime organizations. For this reason, we developed a modular cyber security training programme for the maritime domain called Maritime Cyber Security (MarCy) by implementing Critical Events Model (CEM). Then, we evaluated the MarCy programme by utilizing the Delphi technique with the participation of 19 experts from academia and industry. In this study, we offer cyber security training for seafarers and office employees in shipping companies. We proposed eleven elective modules to improve the knowledge, skills, and attitude of learners against cyber risks. The MarCy programme can be implemented by universities, shipping companies, training institutes, and governmental organizations for maritime cyber security training purposes.

Keywords Maritime cyber security · MarCy · Maritime education and training · Delphi · Critical Events Model

1 Introduction

The maritime industry is a vital sector in global supply chains [134]. Currently, ships perform over 80% of the world trade by volume [134]. Modern vessels are equipped with many automation systems to improve safety and efficiency in operations. However, developing technology in the shipping industry also brought along concerns about cyber risks. Several studies revealed cyber threats and vulnerabilities onboard ships [5], with research highlighting how these vulnerabilities may play a significant role in various maritime incidents as well as financial losses [7, 83, 104]. Accordingly, the International Maritime Organization (IMO) took action, aiming to protect ships from cyber threats. The first proposal came from Canada in 2014 against cyber risks onboard. Canada proposed to be developed voluntary guidelines on maritime cyber security [49]. Afterwards, a resolution for shipping companies was adopted by the IMO. Thanks to the proposal of the USA in 2017[55], cyber risk management became mandatory for ship operators [59]. The human element is also a crucial aspect of risk management and should be carefully considered. Today, millions of professionals work in the maritime sector, with only seafarers numbering nearly 1.9 million professionals [13]. Their cyber awareness is crucial and should be reinforced with training for the effective prevention of cyber risks.

Several organizations (e.g. universities, class societies, and training companies) offer maritime education and training for cadets and professionals in different subjects. One of the domains of this training is cyber security. Cyber security training courses are offered because of occurred cyber incidents in the industry and the requirements of class societies,

✉ Aybars Oruc
aybars.oruc@ntnu.no

Nabin Chowdhury
nabin.chowdhury@ntnu.no

Vasileios Gkioulos
vasileios.gkioulos@ntnu.no

[1] Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, NTNU - Norwegian University of Science and Technology, Gjøvik 2815, Norway

Published online: 03 January 2024

flag states, and vetting programmes. Even though role-based cyber security training is suggested in credited guidelines [14, 32, 100, 139], a majority of cyber security training programmes offer generic content, with each participant taking the same content in courses. However, each role in the maritime industry requires specific learning needs for cyber security. For instance, a Ship Security Officer (SSO) who could be responsible for cyber security onboard, should get deeper knowledge about cyber risks compared to a second engineer (2/E) [139]. Not only the crew onboard but also staff in companies may have different necessities. For example, purchasing and Information Technology (IT) departments don't need cyber security knowledge at the same level. Furthermore, the needs of companies are variable. For instance, cyber security requirements in RightShip [115] are unnecessary for a tanker operator. Spending time on getting irrelevant knowledge might be a lost time in business life. Moreover, it might cause conflicts in the minds of attendees.

1.1 Objective, methodology, and novelty

We proposed a modular cyber security training programme for the maritime domain in this study to accomplish the aforementioned issues. The programme was developed using the Critical Events Model (CEM) and was later evaluated through a Delphi technique with the participation of 19 experts from academia and industry. Eleven elective modules were designed for the cyber security training of seafarers and office staff in shipping companies. Moreover, a potential curriculum, instructional strategies, and training materials were proposed in our study. This study also includes discussions of academics and professionals about maritime cyber security training in different dimensions.

1.2 Scope

The study focuses on the development of a modular cyber security training programme for the maritime domain. Even though the programme can be extended with additional modules to cater to various stakeholders in the maritime sector, such as professionals in ports, naval forces, or maritime administrations, this study specifically considers the implementation scenario of cyber security training for seafarers and office staff. The study was evaluated using the Delphi method; however, practical implementation with learner participation was not conducted. The definitions provided by IMO are employed in this study to delineate the terms *seafarer* and *company*. A seafarer is defined by the IMO as "*any person who is employed or engaged or works in any capacity on board a ship*" [48, 58]. The company (also known as ship operator or ship manager) is defined as "*the owner of the ship or any other organization or person such as the manager, or the bareboat charterer, who has assumed the responsibility for the operation of the ship from the shipowner and who, on assuming such responsibility, has agreed to take over all the duties and responsibilities imposed on the company by these regulations*" [60].

1.3 Structure

This article is organized as follows. Section 2 gives background information to readers. Related works in the literature are investigated in Sect. 3. In Sect. 4, the methodology employed in the study is described in detail. Section 5 presents the MarCy programme for maritime cyber security training. The evaluation of the programme and discussions about maritime cyber security training is given in Sect. 6. Finally, Sect. 8 offers a summary and recommends additional research questions for further investigation.

2 Background

In this section, we present a comprehensive discussion and analysis of the current availability of maritime cyber security training. To achieve this, we conducted extensive research, which involved careful examination of relevant academic studies and utilization of search engines to identify institutes offering maritime cyber security education and training to cadets and professionals. Additionally, we sought out guidelines and questionnaires that include requirements and recommendations for maritime cyber security training.

The results of our investigation revealed that numerous training institutes provide maritime cyber security training programmes. However, we observed that some of these programmes lacked sufficient details about their courses. To ensure the quality and relevance of our study, we focused on those institutes that provided comprehensive information, which could be valuable for our research. Furthermore, we took into consideration previous studies that had already referenced certain institutes' training offerings, and we duly reviewed and cited them to avoid unnecessary duplication of analysis. Through meticulous examinations, we thoroughly analysed the objectives, learning outcomes, curriculums, modalities, and target groups of various training and education offerings in the maritime cyber security domain.

Moreover, we extensively reviewed maritime guidelines, paying special attention to their recommendations concerning maritime cyber security training. This process provided us with valuable insights, particularly regarding suitable modalities and curriculums. We have included these insights in our study and recommended them as valuable training materials in subsequent sections.

Lastly, we also examined questionnaires from vetting programmes, which included recommendations or requirements for cyber security training from maritime companies. The

findings obtained from this analysis were instrumental in designing our comprehensive training programme.

In conclusion, our study encompasses a thorough assessment of maritime cyber security training, drawing information from a diverse range of sources. By relying on extensive research and analysis, we have aimed to make a well-informed and valuable contribution to the field of maritime cyber security education and training.

2.1 Training institutes

In this section, institutes providing maritime cyber security training are in place. Relevant institutes were accessed using the ((“maritime”) AND (“cyber security”) AND (“training”)) search string on the Google search engine. Only institutes that have published their training curriculum were considered. The search revealed many institutes offering maritime cyber security training, with a particular focus on training provided by universities in this section. It is important to note that the institutes offering maritime cyber security training worldwide are not limited to those listed in this section.

Solent University offers three courses regarding maritime cyber security. The course of Proficiency in Cyber Security Hygiene [128] takes two hours and is given online. The course is convenient for crew members and shore staff. An introduction, best practices and overview of basic cyber security principles are involved in the course. Phishing attacks, password security, and safe use of the internet are given in this course. Furthermore, best practices defined by the UK’s Maritime and Coastguard Agency (MCA) [43] and Government Communications Headquarters (GCHQ) [41] are offered. Solent University also offers the Ship Cyber Security Officer course [129] to give required knowledge to cyber security officers onboard and key personnel in maritime companies. The course aims to enhance cyber security awareness, and give required knowledge about types of vulnerabilities, types of threats, and risk management, including risk identification, protection and recovery manners. This course also includes best practices defined by MCA and GCHQ. Participants should complete the Proficiency in Cyber Security Hygiene course, before undertaking the course. The last course offered is Cyber Security for Maritime Professionals [125]. It takes three days and is given on-site. The course was developed for crew members and shore staff to improve cyber awareness about attack types, concepts, and techniques. The course also introduces the EU NIS Directive, ISO 27000 standards for information security, computer system design and networks, methods of protecting data, maintaining privacy, and system integrity. At the end of the course, the participants gain CISCO Introduction to Cyber Security certificate.

The Estonian Maritime Academy organized a summer school for maritime cyber security in 2018 [132, 140]. The summer school was suitable for both professionals and researchers from the IT and maritime fields. The course aimed to enhance awareness about cyber threats and vulnerabilities in the maritime industry. An overview of the tools and communications used in the shipping industry and the cyber risks of autonomous ships were given in the summer school. Moreover, the course led to experience sharing among participants. The academy also offers a BSc-level course entitled Introduction to Cyber Security [131]. The objective of the course is to give a cyber security overview and related risks to ships, organizations and individuals. The course is compulsory for cadets in the navigation and ship engineering departments and is elective for students in the port and shipping management department. The course takes a semester to complete and covers the cyber security terminology, main cyber risks and threats, familiarization with relevant guidelines, best practices of cyber hygiene, and ethical aspects of cyber security.

The Norwegian University of Science and Technology (NTNU) in Norway provides a course titled Maritime Digital Security for master students [96]. The course offers an introduction to maritime digital security, handling of digital vulnerabilities, and implementation of cyber risk management. The course is held intensively over two weeks in a semester. Students go through lectures, group work, and simulator exercises. Moreover, students should make a presentation to complete the course. Typical threats and defence techniques, challenges associated with digital security management, and theories related to digital security management and risk management are provided to students in this course.

Plymouth University is another academic institute offering a cyber security course for the shipping industry [135]. The course titled Cyber Security Awareness for Seafarers takes one day and is delivered on the main campus of Plymouth University. In-house training options are also available.

Universities also offer formal education in master’s degrees specifically developed for the maritime cyber security domain. BSA College in Greece offers a Maritime Cyber Security master’s programme [11]. The French maritime academy, Ecole Nationale Supérieure Maritime (ENSM), also offers a master’s programme, entitled Cyber security for Maritime and Port Systems [35]. Relevant maritime regulations and computer networks are available in the curriculums of both programmes; however, other contents are variable. The digitalization of shipping, general principles of computer operating systems & virtualization methods, maritime cyber security reviews, assessments and audits, cyber security principles, and maritime cyber security management systems, are given in BSA College. ENSM provides the contents of basic knowledge and introduction to maritime cyber security, cyber security of tidal power projects, cyber defence including detection, reaction, resilience, cyber security of industrial

systems and components, and integration of cyber security in maritime projects.

The class society, Registro Italiano Navale (RINA), provides a cyber security course for professionals working in the maritime industry [116]. The course aims to improve cyber awareness onboard and to support office staff in establishing procedures and plans. The course is given online but live. The course curriculum consists of risk identification and response, detecting suspicious activities, reporting cyber incidents, understanding preventative maintenance routines, and such.

The Indian Register of Shipping (IRClass) offers Cyber Security Internal Auditor Course for mariners and IT experts [62]. The participants can get sufficient knowledge to be ready to fulfil cyber security requirements in the International Safety Management (ISM) Code. It takes one day to complete the course. The essential topics of the course are ISM code requirements, cyber risks, reference standards, implementation of cyber risk management procedures, and verification of the implementation of such procedures through an ISM internal audit.

The IMO-recognized organization, the Nautical Institute, in collaboration with HudsonCyber offers the course titled Maritime Cyber Awareness for Seafarers [94, 95]. The course is designed for seafarers. It is given online and takes approximately three hours to complete. The course consists of three objectives: rising cyber security awareness in shipping, helping seafarers to identify potential cyber risks in operations, and educating seafarers about reporting cyber incidents. The curriculum of the course comprises the definition and importance of cyber security, cyber threats and risks, human factors, trust factors, identifying and reporting cyber incidents, best practices, and maritime cyber security scenarios.

Maritime Training Services (MTS) [92] also provides an online cyber security training course to familiarize seafarers with cyber threats in the maritime industry and the detection and prevention measures of such threats. To this end, the course developed includes the topics of creating a strong password, phishing attacks, malware hiding e-mail attachments, safe use of social media, and key tips to improve vessel cyber security.

Maritime Trainer offers maritime-related courses to shipping companies. One course offered for seafarers and office staff is Cyber Security [133]. It is given online and takes nearly two hours. The course curriculum includes the core notions of cyber security, cyber systems onboard ships, some types of malware (e.g. spyware and ransomware), phishing attacks, secure passwords, wireless network security, and the importance of the usage of antivirus and firewall software.

Many providers other than the aforementioned are available for maritime cyber security courses. Lee et al. [75] and Lee et al. [76] examined some of them, such as Det Norske Veritas (DNV) [30], LR [80], Aboamare [1], Aspida, CBS [19, 20], JWC International, KR [71, 72], Maritime Institute of Technology and Graduate Studies (MITAGS) [87, 88], SEANET, Ocean Technologies Group (Videotel) [99]. However, some of them (e.g. CBS, MITAGS, ASPIDA, and JWC International) might no longer offer such courses.

Class societies, universities, maritime associations, and private companies offer online, online live, on-site, and video training for cyber security. The courses are suitable for any professional in the maritime industry, such as IT experts, seafarers, and office employees. The courses typically aim to reply to the necessities of the industry. On the other hand, master's programmes aim to educate domain-specific experts. The training courses are typically given as a lecture modality. Other training methods, such as group discussions, case studies, and demonstrations, are missing in general. Bridge simulators for cyber security training purposes are used in NTNU's MSc-level course and Estonian Maritime Academy's summer school. The summer school also includes practical exercises, such as the use of Open Source Intelligence (OSINT) techniques and hacking tools [79].

Limited information about the curriculum exists for many courses except the master's programme provided by BSA College and the training course offered by RINA. However, RINA's content list is very similar (even the wording used) to suggestions of a guide [14]. The training courses generally include safe use of the internet, phishing attacks, creating secure passwords, ISM Code requirements, and cyber risks of mobile phones and removable media. Additional content is variable by the preference of course providers.

The short courses can be typically completed in a day. Estonia Maritime Academy offers a semester-length course for BSc students. Although NTNU's cyber security course for MSc students is also for a semester, it takes intensively a 2-week period in a semester. Solent University offers three types of courses for different objectives and one of which is to train Ship Cyber Security Officers (SCySO). There is no alternative to this course. In the course of Cyber Security for Maritime Professionals [125], a CISCO Introduction to Cyber Security certificate is issued for attendees. IRClass offers an auditor course and focuses on internal audits for ship and office sides in compliance with the ISM code requirements. Table 1 represents attributes of courses described in this study except for master's programmes. Additional courses and comparisons can be found in the papers of [75] and [76].

The IMO's Resolution MSC.428(98) comprises compulsory cyber security requirements [59], which are mentioned in training courses. However, recommendations from the International Ship and Port Facility Security (ISPS) Code might be overlooked [50]. Similarly, regional requirements and recommendations are often omitted. It is important to acknowledge that covering all official documents issued by flag states is a challenging task in a training programme. Nev-

Table 1 Attributes of courses offered

Provider	Course title	Target group	Modality	Duration	References
Estonian Maritime Academy	Cyber Security Summer School	Professionals from IT and maritime fields	On-Site	5 days	[132]
Estonian Maritime Academy	Introduction to Cyber Security	BSc students in marine departments	On-Site	a semester	[131]
IRClass	Cyber Security Internal Auditor Course	Seafarers and IT experts	Online (Live)	1 day	[62]
HudsonCyber & Nautical Institute	Maritime Cyber Awareness for Seafarers	Seafarers	Online	3 h	[94]
Maritime Trainer	Cyber Security	Seafarers	Online	2 h	[133]
MTS	Cyber Security CBT	Seafarers	Online	2 h	[92]
NTNU	Maritime Digital Security	MSc students	On-Site	a semester	[96]
Plymouth University	Cyber Security Awareness for Seafarers	Seafarers	On-Site	1 day	[135]
RINA	Cyber security in Maritime Industry	Any professional working in the maritime industry	Online (Live)	6 h	[116]
Solent University	Proficiency in Cyber Security Hygiene	Anyone who uses a vessel and IT or OT system	Online	2 h	[128]
Solent University	Ship Cyber Security Officer	Cyber security officers and other key personnel	Online	1 day	[129]
Solent University	Cyber Security for Maritime Professionals	Seafarers and shore-based personnel	On-Site	3 days	[125]

ertheless, it is feasible to include explanations of circulars from select countries, especially those relevant to participants' operations.

The curriculum of many training programmes lacks guidance on developing a cyber security plan, including risk management. Notably, crucial commercial aspects are also missing, such as the cyber attack exclusion clause in marine insurance policies (i.e. CL380), investment recommendations, and vetting requirements. While training providers acknowledge the importance of cyber security in vetting programmes [28, 30, 133], the syllabuses for such training often lack comprehensive information on potential deficiencies, requirements, and recommendations.

Some training courses adopt a role-based approach (e.g. tailored for IT experts, office employees, and seafarers). However, the responsibilities of each employee vary significantly; for instance, an engineer and an officer are accountable for different onboard systems. Therefore, role-based training programmes should be more specific and tailored to the distinct responsibilities of individuals.

Furthermore, the practical application part of training courses, such as updating the operating system, is generally overlooked. During our study, we encountered challenges in addressing these gaps and providing comprehensive coverage of the subject matter.

2.2 Guidelines and questionnaires

The IMO recommends following the Guidelines on Maritime Cyber Risk Management [14] to prevent cyber risks onboard ships [56, 57, 59]. As per the guideline, training and awareness are the key elements to avoid cyber threats and vulnerabilities. Moreover, the guideline states "*an awareness programme should be in place for all onboard personnel according to their role*". Furthermore, training awareness should be given at the appropriate levels to onboard personnel and shoreside personnel. As per the guideline, marine human resource managers should be responsible, and the safety manager, fleet manager, and training manager should provide the required support for crew cyber risk management training. The awareness programme should cover maintenance routines (e.g. antivirus, patching, and backup), e-mail risks (e.g. phishing attacks), risks related to the use of the internet (e.g. social media and cloud storage), risks of the use of own devices (e.g. removable media), risks related to publicly available geolocation data, risks of working third parties alone (without supervision), procedures for the use of third parties' removable media onboard, reporting procedure of cyber incidents, improving awareness about the impact of cyber attacks on safety and operations of the ships, and safeguarding passwords.

The Cyber Security Workbook for on Board Ship Use [139] includes recommendations for the training of seafar-

ers. Cyber security training is also suggested to the office staff who frequently visit ships, such as superintendents. Role-based cyber security training is suggested in the workbook and the mutual parts in the training of seafarers and office staff visiting ships should comprise the use of ship business network, recognizing malware attempts, safe use of the internet including phishing attempts via e-mails, safe file sharing onboard, cyber risks posed by ship visitors, the use of personal devices onboard, safekeeping passwords and sensitive information, the procedures for the use and update of software including antivirus, secure remote connection for software assistance, response plan including reporting procedure. The seafarers should be also aware of signs of a potential cyber incident, such as slow systems, network connectivity problems, changes in software settings, software errors and crashes, and unexpected changes to passwords. The workbook also gives detailed information about the evaluation of crew, designing a training programme, and cyber security drills.

The Implementation Guide for Cyber Security on Vessels [32] published by Digital Container Shipping Association (DCSA) states two types of training. One of which is generic cyber security training for all crew members. This training may include basics of cyber risks onboard, such as phishing attacks and the dangers of using memory sticks. Another training is regarding incident response for the appropriate crew members. The training content could be tailored role-based. The context may include contacts, forensics, reporting, system recovery, restoration, and such.

The Guide for Cyber security Implementation for the Marine and Offshore Industries [2] published by the American Bureau of Shipping (ABS) includes explanations and requirements for the cyber security class notations, such as CS-System, CS-Ready, CS-1, and CS-2. The CS-1 and CS-2 are regarding the companies and request documented records for cyber security training concerning cyber hygiene and support of specialized cyber security functions. Specialized cyber security training other than generic is also requested. For instance, the training for IT and Operational Technology (OT) staff should involve the impacts of disruptions of critical IT and OT systems on personnel and environmental safety.

The Guidelines on Maritime Cyber Safety [63] published by IRClass provides information and requirements for the cyber security class notations titled Informed Cyber Safety (CyS-I) and Advanced Cyber Safety (CyS-II). IRClass expects training to improve cyber awareness. The employees should be trained initially and periodically. Training requirements for cyber safety, such as internal threats, lessons learnt, maintenance routines (e.g. patching and updating), backup and incident response procedures, and external cyber information should be identified. The employees should be notified about updated information on cyber safety. Senior management should be trained about the impacts of cyber incidents on legal and business dimensions.

Cyber security training for seafarers is verified in the vetting inspections by vetting inspectors, including Ship Inspection Report (SIRE) and Chemical Distribution Institute (CDI) inspections. As per the CDI questionnaire [21], the crew should be trained on company procedures to prevent cyber risks, including the use of memory sticks and personal devices, the limitations on the use of equipment, and response procedures in case of a cyber attack. Training films should be shown and crew-specific training should be provided as per the SIRE questionnaire, however, no content suggestion for training is in place [100].

The suggested training contents in the guidelines are typically based on cyber awareness and IT security. Phishing attacks, creating a secure password, and secure use of memory sticks and the internet are highlighted. The importance of crew-specific and periodic training is emphasized. Drills are suggested, but details regarding drills are too limited. One of the important roles in our study is Cyber Security Officer (CySO) and is well defined with potential responsibilities in [47]. According to the guide, the CySO can be assigned to the company office, ship, or both sides, depending on the type of the ship and the fleet size. IRClass also underlines SCySO and Company Cyber Security Officer (CCySO) in its guide [63]. Thus, we also decided to identify two roles as CCySO and SCySO in our study. [65] focuses on a risk assessment for shipboard OT systems, including communication, navigation, cargo management, and machinery systems. The guide is significant to understand potential risks onboard. All such guidelines [14, 32, 37, 47, 61, 65, 86, 139] highlight the importance of awareness to prevent cyber risks, and effective training is strongly suggested for crew and office employees. Moreover, such guidelines look from a broad perspective and give information in technical and procedural dimensions regarding maritime cyber security. Not only guidelines mentioned but also the book written by Kessler and Shepard [70] explains different aspects of maritime cyber security in detail, such as the basics of cyber security, case studies, and strategies for maritime cyber defence. [14] and [139] propose a detailed content list for the training. We took into consideration the contents of such sources while preparing our training curriculum. Several checklists are also offered by [139] to verify the effectiveness of the training. Sources mentioned here don't explicitly reply to questions regarding the training of who should give, how should be given, how long should take, and how often should be repeated. All materials mentioned in this section can be used as training material in a maritime cyber security course.

3 Related work

In this section, we reviewed scientific papers and research projects related to maritime cyber security training and education. We used search string ((“maritime”) AND (“cyber security”) AND (“training”)) to identify relevant studies in the literature. The literature review was conducted using reputable digital scientific libraries, including the Institute of Electrical and Electronics Engineers (IEEE) Xplore, ScienceDirect, SpringerLink, and the Association of Computing Machinery Digital Library (ACM DL). As Google Scholar and ResearchGate provided relevant search results from other scientific databases, we also utilized them. The selection of publications was based on a sequential review of the title, keywords, abstract, conclusion, and the full text of the publications. Furthermore, to access additional publications, we reviewed the bibliographies of the selected publications for back tracing. Citavi software [81] was used to extract data from the articles and manage the acquired knowledge. Objectives, learning outcomes, modalities, curriculums, target groups, advantages and drawbacks of training proposals were extracted. Findings collected in the literature review were later used to design MarCy training programme. Moreover, methodologies for developing a training course were investigated to determine the best method for our research objective. To the best of our knowledge, there are currently no other programmes specific to maritime cyber security training in the literature. That being said, a number of awareness and training activities for maritime and maritime security have been proposed over the years.

The International Association of Maritime Universities (IAMU)’s research project, Addressing Cyber Security in Maritime Education and Training (CYMET), aimed to enhance cyber awareness in the maritime industry through education and training [4]. In the context of cyber security, the training necessities of seafarers were evaluated and recommendations for maritime education and training were provided. Web-based training was suggested through two platforms (i.e. Moodle and Itslearning). The learning package consisted of seven lessons, such as introduction, understanding cyber threats, awareness across the organization, elements of cyber security management, good practices, rules, standards and guidelines, and examples from real life. The package also included an extension with lessons on network integrity, Global Positioning System (GPS) jamming and spoofing attacks, and safe information exchange. Their web-based learning course was tested by a pilot group involving cadets in the project partners. After completing the course, feedback was received by answering several questions. The received replies revealed that the developed course was effective and interesting for the attendees.

Lee et al. [75] offered a training course for the SCySO. Their course proposal comprised a curriculum of 16 h (two days). The curriculum included 23 sections, such as IMO and vetting requirements (i.e. RightShip and Tanker Management and Self Assessment (TMSA)), recent incidents, roles and responsibilities of SCySO, risk assessment, and good practices. The training methods were lectures, presentations, group discussions, and case studies.

Lee et al. [76] proposed cyber security familiarization training for all seafarers. According to their proposal, the training should be added in “Section A-VI/6 Mandatory minimum requirements for security-related training and instruction for all seafarers” in the Standards of Training Certification and Watchkeeping (STCW) Code [52]. The curriculum should cover various aspects, including types and principles of cyber threats, kinds of cyber attacks, the technology of target systems, networks, and equipment, assessment of cyber risks, methods to mitigate cyber risks, development of contingency plans, and best practices based on actual incidents.

Kuhn et al. [73] explored a cyber security exercise at the North Atlantic Treaty Organization (NATO) Centre of Excellence, where participants faced maritime cyber scenarios to assess risk perception and response. Key findings: 1) Group risk perception was effectively evaluated by aligning risk with sector guidelines in a group setting. 2) As incidents escalate, those with public/military experience and mixed cyber security expertise prioritized private sector responsibility and visibility but not urgency. The exercise aided robust cyberspace operations, emphasizing risk assessment’s crucial role. Successful small-scale trials offered capacity-building insights and highlighted the need for joint response to maritime cyber incidents.

Adams et al. [3] reviewed current port security approaches and the cyber-physical security threat, assessing how new systems like Scalable multidimensionAl sitUation awaReness sOlution for protectiNg European ports) SAURON could reduce vulnerabilities. The SAURON hybrid situational awareness tool was developed to detect combined physical and cyber attacks, providing decision-makers with integrated situational awareness and supporting effective countermeasures. The paper emphasized the benefits of such approaches and highlighted the need for security technologies to be complemented by effective processes and personnel with appropriate training. Multidisciplinary training is crucial in combating complex cyber-physical security threats. The study demonstrated how industry and academia-developed technologies can enhance port security, emphasizing the importance of training and awareness in addressing these challenges.

Odessa Maritime Academy is actively involved in the “Trainings in Automation Technologies for Ukraine” project, focusing on modern technologies and cyber security implementation in the maritime field. Shapo and Levinskyi [120] highlighted the need for deepening IT learning in vari-

ous areas like data transfer technologies, computer control systems, and remote control protocols. Additionally, the significance of cyber security education and e-learning technologies was emphasized. The university had well-equipped labs and an e-learning system to facilitate students' access to teaching materials. Courses cover disciplines related to the mentioned areas, benefiting at least 200 students annually. The author possesses experience in industrial cyber security devices adjustment and integration, enhancing the effectiveness of training. The potential audience includes numerous crewing and shipping companies in the region, given Ukraine's considerable seafarer population.

Hopcraft [44] emphasized the link between seafarer training and maritime safety, advocating the development of standardized digital competencies for all seafarers. The complexities of maritime operations and various levels of responsibility make creating standardized competencies challenging. Three levels were identified: Support, Operational, and Management, each requiring specific cyber risk management competencies. Equipping seafarers with appropriate digital competencies ensured awareness of digital system risks and the ability to respond effectively. The NIST Cybersecurity Framework's core functions (Identify, Protect, Detect, Respond, and Recover) were applied to these levels to guide organizations in understanding required competencies. Overall, this paper aligns NIST framework with seafarers' roles at different levels to define essential cyber security competencies.

Olivier et al. [66] presented a high-end hybrid cyber range for port cyber risks awareness and training, focusing on a specific port use-case and achieved results. The Cyber-MAR project demonstrated the topology of a port's critical infrastructure with real cyber-physical systems and devices. The cyber range aimed to simulate cyberattacks to detect, mitigate, and train personnel for crisis management. During a pilot demonstration, the importance of dynamic prevention and reaction measures was emphasized. The Cyber-MAR H2020 project's main objective was to develop innovative environments to simulate realistic cyberattack scenarios and train personnel. The project included a Training Layer with a Learning Management System (LMS) module to improve training performance and experience, providing course catalogues, assessments, and individualized assignments.

Lovell and Heering [79] summarized the findings in the Exercise Neptune organized by Tallinn University of Technology (TalTech) in 2018. The master's students and PhD candidates attended the exercise. A full mission bridge simulator was used in the exercise. The study uncovered that daily orders and confidential orders could be found on Twitter, and NATO warships could be tracked using social media platforms (e.g. Facebook, Twitter, and Snapchat). The study revealed the importance of cyber awareness, training, and misuse of social media at sea. The paper also uncovered that individual information breaches could lead to the whole landscape which might be exploited by malicious actors.

Bacasdoon and Bolmsten [10] investigated four maritime education and training institutes (METI) offering maritime cyber security courses to seafarers. A total of 29 knowledge items and 16 skill items have been provided by four METIs. The courses have been given online or blended (i.e. the combination of online and on-site training). One of the METIs has focused on improving only knowledge. The others have aimed to improve the knowledge and skills of the attendees. All METIs except one have made a test to assess participants after the completion of the course.

Potamos et al. [111] introduced a maritime cyber range training environment designed to simulate offensive and defensive actions in maritime cyber security. The environment included various components like navigational, information, and telecommunications systems, as well as networks and Supervisory Control and Data Acquisition (SCADA) systems. It enabled scenarios such as vulnerability testing, penetration, exploitation, traffic eavesdropping, Global Navigation Satellite System (GNSS)/Automatic Identification System (AIS) spoofing, navigation takeover, and signal intelligence. The cyber range could simulate or emulate Information and Communication Technologies (ICT)/OT systems, providing a realistic setting for cyber security training and research. It aimed to improve situational awareness for ship crew members and onshore operators, aligning with cyber security initiatives and regulations in the maritime domain. Overall, the maritime cyber range contributes to the enhancement of maritime cyber security.

During the literature review, it was seen that developing a methodology for designing a training programme attracted the attention of many researchers. Several models have been proposed to develop a training course [9, 16, 18, 42, 74, 85, 93, 103, 110, 113, 119, 130]. Moreover, review studies for such models and methodologies are available [24, 33, 98].

Ornstein and Hunkins [103] suggested six steps for curriculum design, such as considering curriculum assumptions regarding objectives, participants' needs, various design components and their organization (e.g. content), sketching out design components, cross-checking design components, and sharing the curriculum design with a colleague. Aris et al. [9] proposed a framework for assimilating multidisciplinary programmes in the curriculum structure. The proposed model in the study consists of four stages, such as the identification of elective courses, discussion with faculties and branch campuses, marketing and promotion, and assimilation in curriculum review and development of the new programme. Another model, the High-IMPACT Training Model, was proposed by Sparhawk [130]. The High-IMPACT consists of six steps, such as identifying training needs, mapping the approach, producing learning tools, applying training tech-

niques, calculating measurable results, and tracking ongoing follow-through.

Chowdhury et al. [22] proposed a framework for modelling cyber security training exercises based on concepts of personalized learning theory. The framework uses a revised, five-step ADDIE model for the analysis, design, development, implementation, and evaluation and feedback components. The main purpose of this framework is to tackle the issue of training offerings often being considered not engaging by participants. The authors propose a solution that accounts for the preferred training method, and contents, and conducts thorough evaluation and feedback collection. To account for the participants' requirements and preferences when it comes to training, trainees are involved in all phases of development. This is mainly achieved via feedback collection.

The training models reviewed generally consist of three mutual dimensions, including identifying the needs, building a curriculum, and verification of the model. Several ways are proposed for the verification of a training model. For instance, implementation primarily on a pilot group, discussion with colleagues, or assessing the participants' performance.

As observed, the models for developing a training course are typically proposed for formal education at different levels (e.g. high school or undergraduate studies). Training for professionals is typically not mentioned as an application area of the methodologies in the analysed studies. This represents a significant challenge in the cyber security awareness and training domain, as training professionals require additional consideration, and the previous models would need to be modified and validated for the training of professionals.

4 Methodology

Several models for designing and developing training have been proposed over the years. The Critical Events Model (CEM) [93], initially developed in 1965 under the title "Process of Training" by Leonard Nadler, in 1982, stands out as one of the most well-established and thoroughly described methods in training design. It is also commonly referred to as Nadler's Model [36]. The CEM provides a comprehensive approach to designing any types of training courses, applicable not only to formal education but also to the diverse training needs of various organizations. Its versatility makes it particularly suitable for industries experiencing rapid changes [93]. As of now, the STCW does not include any specific requirements or recommendations to enhance the cyber awareness of seafarers. Consequently, seafarers usually receive cyber security training during their professional careers. To address this gap, our study has incorporated the CEM with several modifications, including the addition of a modular approach and changes to the evaluation step.

In the modular training approach, relevant parts of a training structure are offered to learners by considering personalized training needs. This approach has been performed over the years for different training needs [27]. It is especially effective for vocational training [38]. Given that only required knowledge is provided to attendees by considering their learning needs, it does not cause lost time in business life. That is why modular training is a cost-effective method and can be given online, as well [123]. It provides flexibility to the training designer and learner. The designer can offer new qualifications for trainers by adding new modules, so changing training needs of the industry can be simply responded [38].

As mentioned in Sect. 3, credited organizations in the maritime industry [14, 32, 100, 139] suggest role-based cyber security training. To respond to this recommendation, we sought to bring a modular approach to the MarCy programme. This allows professionals in the maritime domain to take only the required modules of the training based on their roles and responsibilities. By developing modules, the training needs of any professional in the maritime domain, such as seafarers, office staff, port employees, and navy personnel, can be met through specialized cyber security training. In other words the application scope of the programme is expanded. To bring a modular approach to MarCy, we slightly modified Step 1 (i.e. Identify the Needs of the Organization) and Step 3 (i.e. Identify Learner Needs) of CEM. Similar to CEM, MarCy also aims to define the organization's needs in Step 1. However, in MarCy, these needs concurrently define the training modules. In Step 3, MarCy, like CEM, analyses the specific training needs for each role. Additionally, in MarCy, roles and training modules are matched at this step.

In addition to the mentioned modifications to incorporate a modular approach into MarCy, another change was implemented in Step 9 (i.e. evaluation and feedback). The CEM includes a self-evaluation phase, which is performed after each step by discussing with internal and external experts. In practice, this translates to conducting a minimum of eight meetings with experts for the evaluation of a training programme under development. As explained in Sects. 6.3 and 6.7, the number of experts on maritime cyber security globally is still limited. Moreover, arranging meetings with selected experts would prove to be another challenge, both in terms of scheduling and due to time restrictions for training development. For these reasons, we replaced the self-evaluation phase of CEM with our evaluation approach (i.e. Step 9: evaluation and feedback) as described in Sect. 5.9. Simply, while CEM mandates the implementation of the "evaluation and feedback" step after each step, MarCy does not require this. Unlike CEM, MarCy programme, already designed with expert input, enables the enhancement of training effectiveness through simpler modifications tailored to the unique needs of learners. This is achieved by solic-

iting opinions exclusively from internal stakeholders. Our proposed approach still relies on feedback from relevant stakeholders, but it targets only internal stakeholders to the training, such as learners. This approach facilitates data collection and also ensures that the developed training is well-tailored and targeted to training participants.

The objectives of the other steps in MarCy align with the objectives of CEM, however, these other steps are individually applied for each training module in MarCy. Consequently, we propose MarCy programme for maritime cyber security training as represented in Table 2, outlining the implementation phases.

The MarCy programme comprises a total of nine steps. Additionally, the Delphi technique was performed to evaluate the effectiveness and usability of the MarCy programme by considering the needs of maritime cybersecurity training programmes, as illustrated in Fig. 1. In other words, Delphi was solely performed to evaluate the MarCy programme in our study. Course designers don't have to implement Delphi while following the MarCy programme.

The Delphi technique is considered in the literature as a well-suited research instrument to obtain judgement and opinion on incomplete knowledge about a problem or phenomenon [124]. The method generally comprises an iterative process with the goal of collecting feedback on a given topic from a selected, anonymous panel of experts on a topic. Recent adaptations of the method allow for additional flexibility in its implementation. The decision of using the Delphi method as a validation technique for the MarCy came from its ability in collecting weighted feedback from the panel of experts and allow for open debate, without requiring practical methods of evaluation, such as experimentation. The panel was selected based on stakeholder analysis for cyber security training for the maritime sector, with the goal of finding a sufficient amount of experts for each of the following profiles;

- academics who work in the field of maritime cyber security;
- senior industry experts who are responsible for maritime training, including maritime cyber security training;
- senior industry experts who are responsible for the Safety Management System (SMS) of companies, including maritime cyber security policies and procedures.

A total of 37 invitations were sent to relevant stakeholders. The final selection came down to 19 participants with their details represented in Table 3. Some of the academics and experts in our group have a background in sea service as a master, officer, or engineer.

Two rounds of Delphi were conducted in total, with additional questionnaires answered by participants who could not participate in the previous rounds. While Appendix 1 presents the fundamental questions, it's important to note that the discussions in the Delphi rounds extended beyond these specific inquiries. A total of 7 h were spent during the discussions of the two Delphi rounds. The remainder of the Delphi method consisted of the activities listed below:

1. Establish a problem statement—The problem statement represents the general question that will be central to the topics discussed during the process. In our case, the problem statement is the following: *How can a programme for maritime cyber security training be developed in a way that addresses the limitations of current offerings?*
2. Appointing a facilitator/s—The facilitator had the responsibility and was in charge of the following activities: coordinating each round of the Delphi method, analysing the results of the rounds disseminating a report of the results of each round of Delphi to the participants, summarizing the final results and disseminating the final report and programme to the participants. Two facili-

Table 2 Phases of the MarCy training programme

Phase	Function
Step 1: identify the needs of the organization	Modules are identified by considering the needs of the organization
Step 2: specify job performance	Roles and responsibilities of employees are investigated
Step 3: identify learner needs	Modules are mapped with roles by considering responsibilities
Step 4: determine objectives	Objectives and the learning outcomes of the modules are identified
Step 5: build curriculum	A curriculum is created for the modules
Step 6: select instructional strategies	Instruction modalities are identified
Step 7: obtain instructional resources	Training resources required are analysed
Step 8: conduct training	It is identified how to perform the training
Step 9: evaluation and feedback	The effectiveness of the designed training is verified

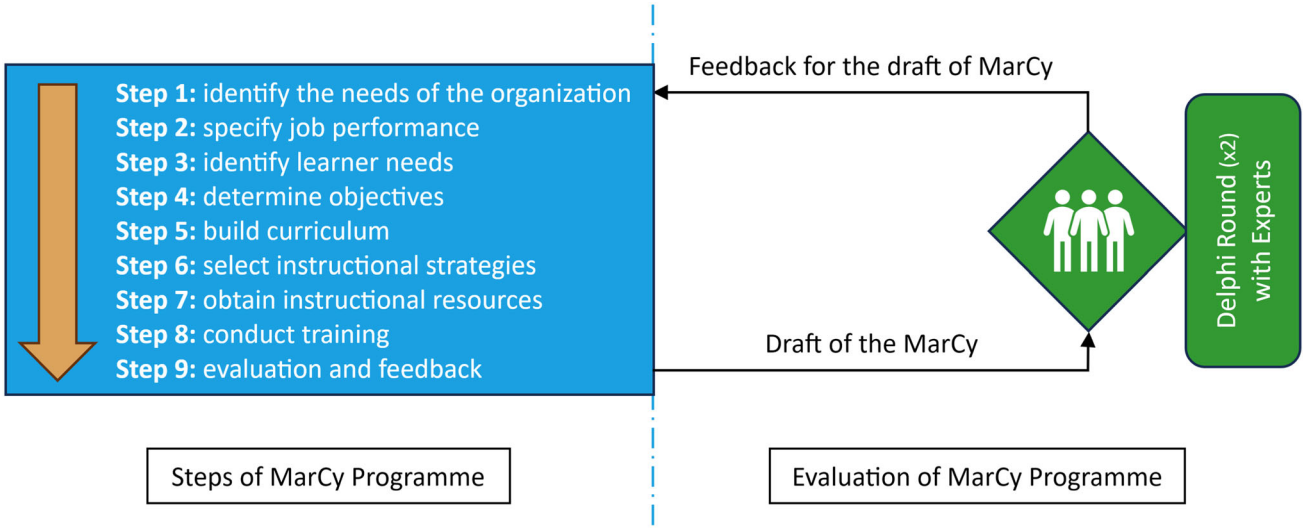

Fig. 1 Graphic Illustration of the Evaluation Process of MarCy Programme

Table 3 Profiles of the participants

Number	Participant profile	Job title
9	Academics in maritime cyber security	Research officer
		Research fellow (PhD candidate)
		Researcher (PhD)
		Assistant professor (PhD)
		Full professor
5	Experts in maritime cyber security	Assistant director in a research centre at a university
		OT cyber security officer in a shipping company
		Managing director in a maritime cyber resilience centre
		Lead cyber security specialist in a class society
		Advisor global support in a marine underwriter
2	Experts in maritime	Marine and HSSEQ manager in a shipping company
		HSEQ superintendent in a shipping company
2	Experts in maritime training	Training superintendent in a shipping company
		Training manager in a shipping company
1	Academic and expert in maritime cyber security	Full professor and independent consultant

tators were chosen. One was in charge of moderating the discussion during the Delphi, while the other had note-taking duties. Both facilitators were in charge of analysing the data collected during the Delphi rounds, to complete reports for each round.

3. First round of Delphi—A first round was conducted with four academics working on maritime cyber security, focused on collecting feedback on current maritime cyber security training, as well as initial feedback on the MarCy programme. The round also served as an evaluation of the format of discussion to be used during the next Delphi discussions. The first round took around two hours to complete.
4. Second round of Delphi—One more round was scheduled with additional experts from both industry and academia. Due to the number of participants, the round was split into two sessions on different dates. 13 participants joined the first session, while 10 the second session. Participants joined the sessions based on their availability, with a majority of participants joining one of two sessions, while a minority joined both sessions. 17 unique participants attended in total, between the two sessions. Both sessions focused on current maritime cyber security training and feedback on the MarCy programme, although each focused on a different set of questions on each of the topics. In total, the two sessions took over five hours to complete.

Table 4 Main topics of discussion of during the Delphi, with a description of each

Topic	Content
Discussion on maritime cyber security training	Main considerations that distinguish maritime cyber security training from other cyber security disciplines; Recommended training methods for maritime cyber security; Limitations of current offerings in maritime cyber security training; How to address such limitations; Methods & Criteria for evaluating maritime cyber security training; Additional considerations/comments
Feedback on the MarCy programme	Evaluation of addressed training needs & requirements; Evaluation of identified roles, training modules, training content, and the association between roles and training modules; Evaluation of prerequisites; Overall evaluation of programme's structure, objective and usability; Additional considerations

5. Questionnaire—After completing the two rounds of the Delphi, a questionnaire was sent to selected participants who were not available during the previous rounds. The questionnaire summarized all the topics discussed during the previous rounds of Delphi. Together with the questionnaire, a report summarizing the results of the previous Delphi discussion was sent to participants. Despite our endeavour, we were not able to receive any input through the questionnaire for our study.
6. Conclusion of the Delphi method—After collecting feedback from all participants, a final report summarizing all the inputs and conclusions reached by participants was completed. The report was shared with all participants for validation and recommended changes and considerations were later integrated into the programme.

Each round of Delphi was conducted digitally, via an online video-conferencing tool. A video and written transcript of each meeting were recorded. No information regarding participants' identities or companies was disclosed in the reports. The rounds were all structured in two parts, one focused on collecting feedback on current maritime cyber security training offerings and their limitations, and the second part focused on feedback on the proposed programme. An initial broad discussion on maritime cyber security training was conducted to allow participants to discuss the State-of-the-Art (SoA) on maritime cyber security training, highlight current limitations, as well as recommend solutions to these limitations. Table 4 provides a description of the content of each of these parts.

5 MarCy: maritime cyber security training programme

In this section, we discuss in detail the MarCy programme for maritime cyber security training. The discussion is structured in sections, each focusing on a specific step. Here, we elaborate on the process by providing an example application field: the training of seafarers onboard and office staff in companies.

5.1 Identify the needs of the organization

The objectives of this step are to identify the nature of the problem [93]. In the first step, the training needs of the company should be identified, such as international regulations and class notations. Determined training needs identify the required training modules. Module codes and titles should be also specified in this step.

A company may need to train seafarers employed and office employees to improve their cyber awareness because of potential and occurred cyber incidents in the industry, cyber threats in threat landscape reports, and revealed cyber risks in studies. Furthermore, vetting, flag state, and class society requirements or recommendations may force companies to improve the cyber awareness of professionals employed.

The vetting programmes play an important role in the business life of a shipping company. The SIRE and CDI inspections force tanker management companies to provide sufficient training for seafarers employed to improve cyber awareness [106]. The TMSA requests tanker management companies to promote cyber awareness of ship and office personnel [102]. The RightShip recommends dry bulk management companies train seafarers and improve cyber awareness [115]. The next regime of the SIRE, SIRE 2.0, also will force tanker management companies to train seafarers employed for cyber security issues [101]. The SIRE 2.0 is expected to become operational in 2023.

The class societies, such as the ABS [15], Bureau Veritas (BV) [117], DNV [31], IRClass [63], Korean Register (KR) [26], Lloyd's Register (LR) [118], and Nippon Kaiji Kyokai (ClassNK) [97], offer cyber security class notation for shipping companies. The expectation of class societies for the notation may include training of seafarers employed for cyber risks onboard ships (e.g. ABS [2], ClassNK [23], DNV [29], and IRClass [63]).

The Singapore Registry of Ships (SRS) provides voluntary notations for Singaporean ships, such as green, cyber, smart, and welfare notations [90]. Cyber notation is divided into three levels, including SRS Cyber Basic, SRS Cyber Intermediate, and SRS Cyber Advanced. The proof for the training of the crew is requested for any type of cyber notation [91]. Phishing attacks, suspicious e-mails, and insecure URLs shall be discussed in the training courses [91].

Table 5 Training needs and modules

Potential training needs of a company	Modules and specifications
Basic cyber risks and mitigation measures, such as malware infection risks, port security (e.g. RJ-45 & USB), safe use of the internet, and creating a secure password	M1: Basic cyber security
Advanced knowledge of cyber security such as IT/OT systems differences, malware types, stages of cyber incidents, threats actors and their motivations	M2: Advanced cyber security
International and regional regulations and recommendations	M3: Regulatory requirements
SIRE, SIRE 2.0, CDI, TMSA, or RightShip requirements	M4: Vetting requirements Specify: (e.g. TMSA)
Cyber vulnerabilities of bridge systems, cargo handling and management systems, communication systems	M5: Critical deck systems
Cyber vulnerabilities of propulsion and machinery management and power control systems	M6: Critical engine systems
Cyber vulnerabilities of access control systems, passenger servicing and management systems, passenger-facing public networks, administrative and crew welfare systems	M7: Other critical systems
Potential investments (e.g. ISO standards and flag state and class notations)	M8: Cyber security investments Specify: (e.g. DNV Cyber Secure and SRS Cyber Basic)
Getting practice, such as performing checklists, procedures, and policies operating system and antivirus updates	M9: Cyber security practices Specify: (e.g. Windows 10 and Kaspersky Total Security) Provide required checklists, policies, and procedures from the company's SMS
Getting knowledge to manage cyber security matters in the company, such as developing a cyber security plan, risk management, and cyber security drills	M10: Cyber security management Provide risk management procedures from the company's SMS
Getting advanced technical skills such as intrusion detection, and use of cyber security tools	M11: Advanced skills Specify: (e.g. Kali Linux)
Additional needs	Additional modules

As per the ISM code requirements, each company must have a cyber risk management section in their SMS. This requirement has been verified in Document of Compliance (DOC) audits in the companies' offices, and in Safety Management Certificate (SMC) audits onboard ships since 2 January 2021. Moreover, as per the IMO guide [50], the Ship Security Plan (SSP) should refer to such cyber risk management procedures in the SMS. Not only current regulations but also forthcoming regulations might need to be known to be ready. In December 2021, the Republic of Korea proposed to be discussed the necessity of developing inclusion for cyber security training for the STCW [51]. The Sub-committee on Human Element Training and Watchkeeping in the IMO was invited to discuss relevant provisions of cyber security-related training for seafarers [51]. As per the IMO, cyber security training is still not a requirement but would be a requirement or recommendation in the near future.

Companies may also need to train crew to be gained technical and procedural practice in the implementation. Moreover, the responsible person may require additional training for effective management of cyber security matters in the company. Last, advanced technical capability, such as the use of cyber security tools, could be required for some dedicated staff in a company.

The typical needs of a company are given in Table 5; however, companies might have additional training needs. In such a case, additional needs of the company should be specified as well as module code and title. Companies may not require all proposed training modules in Table 5. For instance, personnel of a company managing passenger ships don't need to learn cyber security requirements in vetting programmes. Lastly, some modules may need to be specified by considering the company's certain needs, including equipment onboard, class notations, flag state notations, vetting requirements, operating systems, installed software, company SMS, and so on.

5.2 Specify job performance

The objective of this step is to investigate employees' roles and responsibilities [93]. We analysed seafarers onboard and employees on the shoreside of companies. To this end, we perused the SMS of three companies, the websites of several companies, flag state documents, the STCW Convention, the ISM Code, and the ISPS Code. Furthermore, we performed a literature review. Afterwards, gathering data was synthesized and organized.

Each company may have a different organizational schema and identify different responsibilities for each role. Ships

are managed as per national and international requirements. Thus, designing an organization chart and identifying roles for the crew onboard are easier. However, various variations for the organization and responsibilities are existing in the office side. In Sects. 5.2.1 and 5.2.2, a generic viewpoint for crew and shore staff is provided to understand roles and responsibilities. Moreover, the CySO role for ship and office is explained in Sect. 5.2.3.

5.2.1 Seafarers on a typical ship

The crew of a ship can be divided into three categories: master, officers, and ratings. The IMO defines master as "*the person having command of a ship*" [60]. The IMO defines an officer as "*a member of the crew, other than the master, designated as such by national law or regulations or, in the absence of such designation, by collective agreement or custom*" [60]. The IMO defines a rating as "*a member of the ship's crew other than the master or an officer*" [60].

A typical ship can be divided into three departments, including deck, engine, and catering (galley). The master is not involved in any departments. The deck department consists of deck officers and ratings. The deck officers are typically responsible for safe navigation, communication, and cargo operations onboard [126]. The deck officer states chief officer (C/O) (known as chief mate), second officer (2/O), 3rd officer (3/O), deck cadet (D/C) (trainee deck officer). The deck rating depicts bosun (known as boatswain), able seaman (A/B), and ordinary seaman (O/S). The engine department consists of engineer officers, electro-technical officers, and ratings. Engineer officers are typically responsible for the maintenance and operation of the ship's main propulsion and auxiliary systems [127]. The engineer officer state chief engineer (C/E), 2/E (known as first assistant engineer), third engineer (3/E) (known as second assistant engineer), fourth engineer (4/E) (known as third assistant engineer), and engine cadet (E/C) (trainee engineer officer). Electro-technical officers are responsible for monitoring, operation, maintenance, and repair of several systems onboard ship, such as electrical, electronic, and control systems [60]. Furthermore, electro-technical officers should be able to operate computers and computer networks on board ships as per the IMO requirements [60]. Many documents still call electrical officers. However, it was replaced with electro-technical officers as of STCW 2010 [84]. The engine rating denotes fitter (known as donkeyman), oiler (known as motorman), and electro-technical rating. The catering department consists of a cook and a steward. Last but not least, as per the ISPS Code requirement, an SSO must be designated on each ship [54]. The roles and responsibilities of the crew by rank are described comprehensively in [6, 12, 60, 77, 82, 112]. Master, C/O, C/E, and 2/E are at the management level and are called senior officers [77]. 2/O, 3/O, 3/E, and 4/E are at the operational level and are called junior officers [77]. The ratings are at the support level [77]. The crew number has decreased with the effect of technological developments in the maritime industry. Thus, the companies started not to man vessels with a steward, particularly vessels with up to nearly 20 crew members. Each vessel may have a different organizational structure. For instance, the master or C/O is nominated as an SSO in a typical cargo ship. However, a dedicated SSO might be nominated for passenger ships. Another example is gas engineers manned to gas carriers.

Figure 2 represents a typical ship organization chart for cargo ships. A vessel may be manned with more or fewer seafarers. The dark green colour denotes deck officers. The grey colour states deck ratings. The dark blue colour denotes an electro-technical officer and engineer officers. The orange represents engine ratings. The red colour represents ratings in the catering department. The turquoise colour depicts the master. Master is also stated with four circles in the figure. Three circles represent leaders of deck and engine departments (i.e. C/O and C/E). Two circles state officers other than department leaders. A circle expresses ratings.

5.2.2 The departments and individual roles in a typical company

Many departments for a reliable operation serve in a company. Roles and responsibilities of departments and employees in a department are variable by company requirements and management decisions. In a typical company, the claims & insurance department follows and manages claims (e.g. cargo, bunker, charter party, and collision claims) and insurance process (e.g. Protection and Indemnity (P&I) and Hull and Machinery (H&M)) [138]. The IT department is responsible for the maintenance, monitoring, and installation of IT systems, including hardware and software (e.g. switches, routers, laptops, operating systems, and antivirus). The operation department provides voyage management and operational support, such as assigning surveyors for cargo and bunker surveys and arranging fresh water and bunker supply. The chartering department is responsible for the employment of the vessels [40]. The accounting department is responsible for all accounting tasks for each vessel and the company, including settlement of freight and charter accounts, payment of invoices, and settling of accounts for each crew member [121]. The financial department analyses shipping and capital markets, proposes investment ideas, and reviews the company's financial statements [68]. The vetting department takes required actions both for internal and external audit and inspection requirements. The audit and inspection requirements are followed closely. The Health, Safety, Environment and Quality (HSEQ) department is responsible for the development and effective implementation of SMS as per the national (e.g. local laws) and international

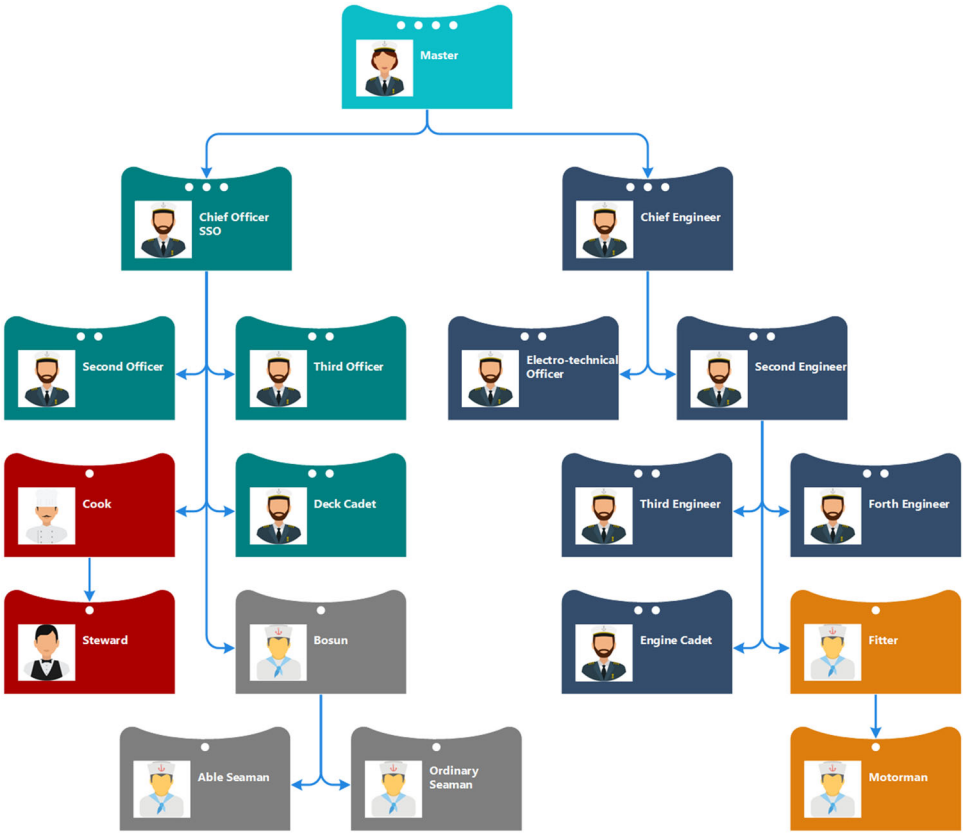

Fig. 2 A typical ship organization chart for a cargo ship

requirements (e.g. IMO requirements), vetting requirements (e.g. SIRE, CDI, RightShip, and TMSA), and standards (e.g. International Organization for Standardization (ISO)). The training department is responsible for the training of crew and office staff. The training programme is published, followed, implemented, monitored, and recorded by national and international requirements, vetting requirements, and findings in audits and inspections. The crewing department is responsible for the initial interview in the crew member and office employee selection. The vessels are adequately manned by the crewing department, considering national and international requirements. The technical department is responsible for the technical support, supervision, and audit of the vessels. The Planned Maintenance System (PMS) is developed and effectively implemented onboard ships. The technical department supports vessels in maintenance and repairs to minimize non-operational time by considering company procedures and national and international requirements. The purchasing department is responsible for the supply of spare parts, provisions, safety equipment, medicines, consumables, slop-chest articles, and so on. The marine department supports vessels with the loading, carriage and discharge of cargoes, and voyage planning [39].

Assigning a DPA is an ISM code requirement and is stated as "*To ensure the safe operation of each ship and to provide a link between the company and those on board, every company, as appropriate, should designate a person or persons ashore having direct access to the highest level of management*" [53]. As per the ISPS Code, a company must designate a Company Security Officer (CSO) at the office for ships who is responsible for monitoring security activities, improving security awareness, ensuring that Ship Security Assessment (SSA) is performed, and such [54]. Managers in the departments have strong leadership skills, capable of managing and motivating staff [39]. Superintendents have strong electronic, electrical, nautical, cargo, engineering, construction, and regulation knowledge based on the department in a company [39].

Figure 3 represents a typical organizational chart for a company. However, companies are allowed to design their organizational structure. Some services can be received from 3rd parties. For instance, a commercial department is unnecessary if the commercial management is offered by an external provider. Each company may call employees in a department with different titles, such as director, manager, superintendent, coordinator, operator, auditor, officer, broker, assistant, accountant, and their variations (e.g. deputy,

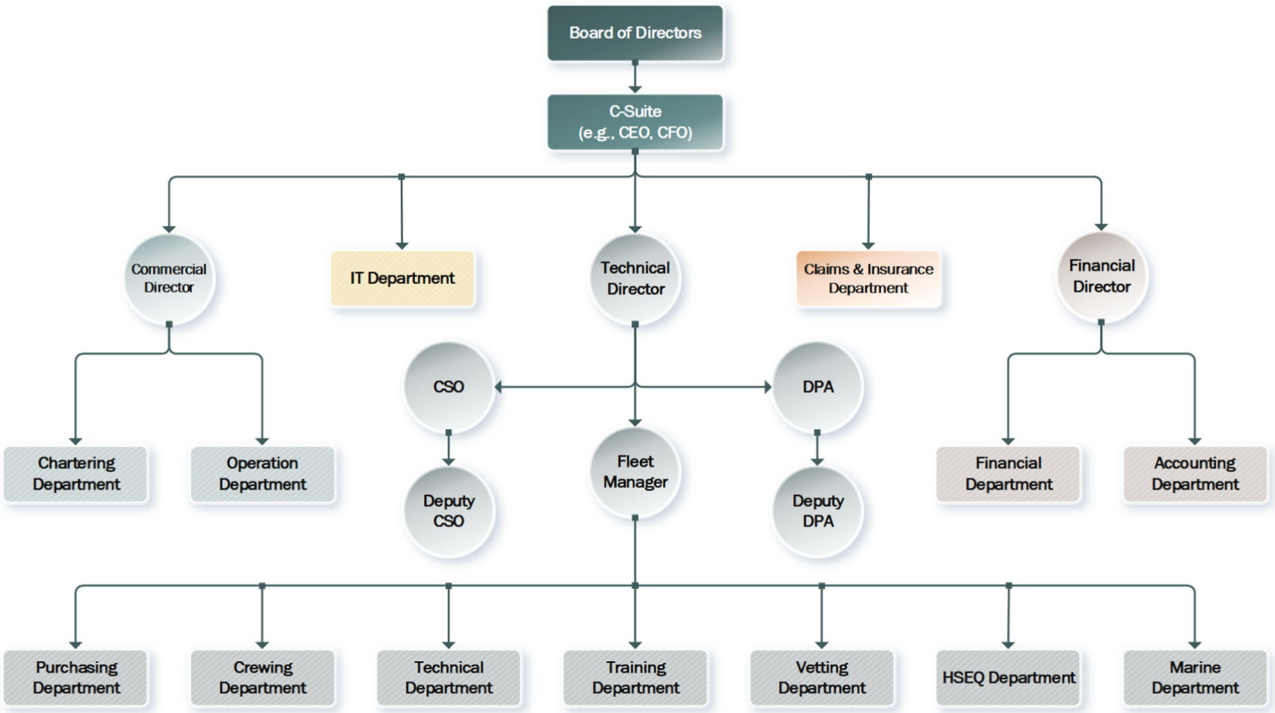

Fig. 3 A typical organization chart in a company

senior, junior). The DPA and CSO are only mandatory roles as per the IMO requirements as aforementioned.

5.2.3 Cyber security officer

Although it is not defined by the IMO, companies may nominate a CySO to their managed ships and/or to the office for the development, management, and implementation of the cyber security plans efficiently. The CySO is relatively a new notion for the maritime industry and may also be called an SCySO [63], Cyber security Representative [2], Ship Cyber Safety Officer [63], Chief Information Officer (CIO) [47], and CCySO [63] in different guidelines. In our study, we use the notions of SCySO and CCySO. CySO depicts both SCySO and CCySO in our study. ABS suggests electro-technical officers and chief engineers to be nominated as the SCySO [2]. We noticed that one of the deck officers is typically assigned as SCySO onboard. On the other hand, IT managers or DPAs are generally assigned as CCySO at the shoreside.

5.2.4 Identification of the responsibilities, ranks, and positions

As aforementioned, in this step, a company should identify the ranks, positions, and responsibilities of the crew and office personnel employed. Tables 6 and 7 represent typical responsibilities for crew and office staff. Such responsibilities were identified by considering Sects. 5.2.1, 5.2.2, and 5.2.3. In this step, the ranks for crew and positions for office staff should also be specified. For instance, a training superintendent may be responsible for training activities in a company.

Some roles (e.g. engineer officers in Table 7) and responsibilities (e.g. marine operations in Table 6) can be grouped if the individuals in such groups have the same training needs for cyber security. For instance, the engineer officers, including C/E, 2/E, and 3/E, could be accepted as a group. Since such ranks work on the same machinery systems onboard. That's why they would have the same training needs for cyber security.

Employees whose responsibilities are not described in Tables 6 and 7, might work onboard or in the office. In such a case, responsibilities for the crew and office staff should be added to the tables and roles should be specified. Lastly, various training modules are shown in Tables 6 and 7. The function of such columns, including training modules, is elaborated in the next step (Sect. 5.3).

5.3 Identify learner needs

The objective of this step is to understand the specific learning needs of roles [93]. The training modules for each specific role are determined in this phase. The training modules in Table 5 are mapped with responsibilities as represented in

Table 6 Responsibilities and positions of office staff

Responsibility	Position (Role)	Training module
training activities	Specify: (e.g. training superintendent)	M1: Basic cyber security
		M3: Regulatory requirements
		M4: Vetting requirements
		M5: Critical deck systems
		M6: Critical engine systems
		M7: Other critical systems
cyber security activities	Specify: (e.g. CCySO)	M1: Basic cyber security
		M2: Advanced cyber security
		M3: Regulatory requirements
		M4: Vetting requirements
		M5: Critical deck systems
		M6: Critical engine systems
		M7: Other critical systems
		M8: Cyber security investments
		M9: Cyber security practices
		M10: Cyber security management
		M11: Advanced skills
IT activities	Specify: (e.g. IT operator)	M1: Basic cyber security
		M2: Advanced cyber security
		M5: Critical deck systems
		M6: Critical engine systems
		M7: Other critical systems
investments and management in marine operations	Specify: (e.g. CEO, CFO, DPA, CSO, HSEQ manager, vetting manager)	M1: Basic cyber security
		M3: Regulatory requirements
		M4: Vetting requirements
		M8: Cyber security investments
marine operations	Specify: (e.g. HSEQ superintendent, marine superintendent)	M1: Basic cyber security
		M3: Regulatory requirements
		M4: Vetting requirements
support activities	Specify: (e.g. purchasing coordinator, accounting manager)	M1: Basic cyber security
additional responsibilities	Specify	Should be selected by considering individual responsibility. Potential module include but are not limited to; M1: Basic cyber security

Tables 6 and 7. The responsibilities of roles can be variable by company preference. That's why modules should be mapped by considering responsibilities instead of roles. Given that responsibilities are already mapped with roles (in step 2 (Sect. 5.2)), the required training modules for each role are unveiled. Mapping modules with the responsibilities of employees could be complicated for some training designers. That's why we also explained an easier way for module selection in Sect. 5.3.1.

After the required training modules are determined, an exam can be given to assess the knowledge of participants. If a participant has sufficient knowledge, it is unnecessary to give him/her such a training module. In this way, the participant doesn't lose time and energy for the module he/she already knows.

5.3.1 The easier implementation for the module selection

In this section, an easier implementation in the module selection is explained for the training of seafarers and office staff. Firstly training needs of a company are determined by considering Table 5. Thus, the required modules are identi-

Table 7 Responsibilities and ranks of crew onboard

Responsibility	Rank (Role)	Training module
navigation, communication, and cargo operations	Specify: (e.g. master and 2/O)	M1: Basic cyber security M3: Regulatory requirements M4: Vetting requirements M5: Critical deck systems
maintenance and operation of the ship's main propulsion and auxiliary systems	Specify: (e.g. engineer officers)	M1: Basic cyber security M3: Regulatory requirements M4: Vetting requirements M6: Critical engine systems
monitoring, operation, maintenance, and repair of electrical, electronic, and control systems	Specify: (e.g. electro-technical officers)	M1: Basic cyber security M3: Regulatory requirements M4: Vetting requirements M5: Critical deck systems M6: Critical engine systems M7: Other critical systems
operation of computer and computer network	Specify: (e.g. electro-technical officers)	M1: Basic cyber security M3: Regulatory requirements M4: Vetting requirements M5: Critical deck systems M6: Critical engine systems M7: Other critical systems
cyber security activities onboard	Specify: (e.g. Ship Cyber Security Officer, SSO, 3/O)	M1: Basic cyber security M2: Advanced cyber security M3: Regulatory requirements M4: Vetting requirements M5: Critical deck systems M6: Critical engine systems M7: Other critical systems M9: Cyber security practices M11: Advanced skills
supporting officers in duties (i.e. ratings)	Specify (e.g. bosun, able seaman, cook, steward, and fitter)	M1: Basic cyber security
additional responsibilities which are none of the above	Specify: (e.g. gas engineer)	Should be selected by considering individual responsibility. Potential modules include but are not limited to; M1: Basic cyber security M3: Regulatory requirements M4: Vetting requirements M5: Critical deck systems M6: Critical engine systems M7: Other critical systems

fied. Then, modules are placed as given in Table 8. In our example implementation, all training modules in the MarCy programme were determined as required. However, all of them might not be required for a company.

Secondly, the roles should be identified for crew and office staff. Typical responsibilities for crew and office staff are given in Tables 6 and 7. The roles should be specified by considering the responsibilities in the tables. As explained in Sect. 5.2.4, some individual roles can be grouped. In further paragraphs, you will find examples for such groups.

In our example implementation, the crew onboard consists of an individual role (i.e. SCySO) and five role groups (i.e. master and deck officers, engineer officers, electro-technical officers, other officers, and ratings). For instance, the mas-

ter, C/O, 2/O, and 3/O were grouped as Master and Deck Officers in our example implementation. Such roles operate the same systems onboard such as navigation, communication, and cargo handling systems [126]. Engineer officers can operate the same systems, such as the main propulsion system and auxiliary systems [127]. The electro-technical officer is an individual rank and can operate electrical, electronic, and control systems, including computers and computer networks [60]. As aforementioned, each vessel may be manned with additional officers (e.g. gas engineer). Thus, we identified another role called other officers in our example implementation. Ratings as the last role was identified for our example. All individual roles and role groups are deployed in Table 8.

In the example, office staff consists of an individual role (i.e. CCySO) and four role groups (i.e. key staff, training staff, IT staff, and other staff). The key staff depicts employees who are responsible for the technical management of ships, such as DPA, CSO, managers (e.g. fleet and vetting managers), and superintendents (e.g. marine and HSEQ superintendents). Key staff also include the top management of the company, such as the Chief Executive Officer (CEO) and Chief Financial Officer (CFO). IT and training staff are other roles in our example implementation. The employees for operational support in other departments, such as accounting and purchasing departments are called other staff in our example implementation. All individual roles and role groups are placed in Table 8.

In the last step, training modules are mapped with roles. Tables 6 and 7 suggest training modules by responsibilities. By considering such suggestions, roles were mapped with training modules as represented in Table 8.

Table 8 Training modules by roles in an example implementation

Module code and title		Crew						Office staff					
		SCySO	Master & deck officers	Engineer officers	Electro-technical officers	Other officers	Ratings	CCySO	Key staff	Training staff	IT staff	Other staff
M1	Basic cyber security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
M2	Advanced cyber security	✓						✓			✓	
M3	Regulatory requirements	✓	✓	✓	✓	✓		✓	✓	✓		
M4	Vetting requirements	✓	✓	✓	✓	✓		✓	✓	✓		
M5	Critical deck systems	✓	✓		✓	✓		✓		✓	✓	
M6	Critical engine systems	✓		✓	✓	✓		✓		✓	✓	
M7	Other critical systems	✓			✓	✓		✓		✓	✓	
M8	Cyber security investments							✓	✓			
M9	Cyber security practices	✓	✓	✓	✓	✓		✓				
M10	Cyber security management							✓				
M11	Advanced skills							✓				

5.4 Determine objectives

The purpose of this step is to identify the specific objectives and learning outcomes for each training module [93]. In our study, each module includes a different objective as represented in Table 9. The learning outcome comprises three components to reach the objectives identified, such as knowledge, skill, and attitude [93]. Knowledge is defined as "*the state of knowing about a particular fact or situation*" [108]. Skill is defined as "*the ability to do something well*" [109]. Attitude is defined as "*a feeling or opinion about something, especially when this shows in your behaviour*" [17].

5.5 Build curriculum

The purpose of this step is to build a syllabus to meet the learning objectives stated in Table 9 [93]. The contents are specified by considering module objectives and desired learning outcomes (i.e. knowledge, skill, and attitude). The contents are divided into two groups: essential and helpful.

Table 9 Objectives and learning outcomes of training modules

Code	Objective	K/S/A	Desired learning outcome
M1	Learners will be familiar with the basics of cyber security.	K	- Learners will have developed a comprehensive awareness of core cyber security matters, including essential concepts, types of cyber incidents, potential cyber risks, and effective mitigation measures
		A	- Learners will be able to demonstrate safe and responsible use of the internet and systems onboard
M2	Learners will have advanced knowledge of cyber security.	K	- Learners will acquire advanced knowledge in cyber security matters, encompassing understanding of attack stages, various types of malware, and insights into malicious actors' behaviours and motivations
M3	Learners will learn international requirements and recommendations for cyber security.	K	- Learners will be able to identify and apply cyber security requirements and recommendations issued by the IMO - Learners will gain familiarity with cyber security-related flag state circulars, enabling them to comply with the relevant regulations and guidelines - Learners will be capable of recognizing potential deficiencies in inspections, and implementing best practices to enhance the overall security posture - Learners will be equipped with up-to-date information on forthcoming cyber security regulations, enabling them to proactively prepare and comply with upcoming changes
M4	Learners will learn cyber security requirements in vetting programmes.	K	- Learners will be proficient in understanding the requirements and recommendations of vetting programmes to ensure adherence to cyber security standards - Learners will be able to identify potential deficiencies related to cyber security in vetting programmes and will be equipped with best practices to address them effectively
M5	Learners will learn cyber risks in the deck systems.	K	- Learners will acquire comprehensive knowledge of cyber risks related to critical deck systems and will be proficient in implementing appropriate mitigation measures - Learners will be capable of effectively handling cyber security incidents related to critical deck systems
M6	Learners will learn cyber risks in the engine room.	K	- Learners will acquire comprehensive knowledge of cyber risks related to critical engine systems and will be proficient in implementing appropriate mitigation measures - Learners will be capable of effectively handling cyber security incidents related to critical engine systems
M7	Learners will learn cyber risks in other systems.	K	- Learners will acquire comprehensive knowledge of cyber risks related to other critical systems and will be proficient in implementing appropriate mitigation measures - Learners will be capable of effectively handling cyber security incidents related to other critical systems
M8	Learners will be able to decide cyber security investments.	K	- Learners will be able to identify and understand cyber security-related clauses in marine insurance policies, enhancing their ability to make informed decisions regarding coverage and risk management - Learners will gain familiarity with various cyber security certifications, such as ISO 27000, and their significance in ensuring a robust security framework - Learners will be equipped with knowledge about cyber notations of flag states and class societies, enabling them to assess their effectiveness for their own company - Learners will be able to develop budgets for implementing cyber security measures and initiatives effectively

Table 9 continued

Code	Objective	K/S/A	Desired learning outcome
M9	Learners will have practical experience in implementation.	S	- Learners will be proficient in performing software and operating system maintenance practices to ensure a secure and up-to-date cyber environment
			- Learners will gain practical experience in using various cyber security tools and applying them appropriately for enhanced system protection
			- Learners will develop effective information sharing and communication skills to foster a culture of cyber security awareness within their organizations
			- Learners will be proficient in public speaking and presentation skills, enabling them to effectively communicate cyber security concepts and strategies to diverse audiences
		A	- Learners will gain expertise in performing company procedures, including the incident response plan, to ensure swift and effective action in the event of cyber security incidents
M10	Learners will be able to manage cyber security issues in a company.	K	- Learners will be familiarized with valuable resources and materials for continuous learning and improvement in cyber security practices
			- Learners will be proficient in designing comprehensive cyber security training programmes to educate and empower employees in safeguarding against cyber threats
			- Learners will be capable of making informed recommendations in developing and implementing a robust cyber security plan tailored to their organization's needs and risks
			- Learners will develop skills in risk management to proactively assess and address potential cyber security threats and vulnerabilities
		A	- Learners will be proficient in evaluating the effectiveness of cyber security procedures and making necessary adjustments to enhance their efficiency
M11	Learners will have advanced technical skills.	S	- Learners will gain hands-on experience in using penetration testing tools to identify vulnerabilities in their systems and networks, enabling them to address potential weaknesses effectively
			- Learners will be able to select and utilize security software to protect their systems and networks from cyber threats effectively
			- Learners will develop system administration skills, ensuring they can maintain a secure and well-protected cyber environment for their organizations

K: Knowledge S: Skill A: Attitude

Essential content is required to meet objectives [93]. Helpful content is supplementary to essential content [93]. We offered a content list for each training module as represented in Appendix 1. While designing the curriculum for modules, we perused current training courses, guidelines, questionnaires, and previous studies mentioned in Sect. 2.

The order of the modules and curriculum items is also decided in this phase [93]. Module 1: Basic Cyber Security is the required module to be taken before any other desired module. Other conditions are represented in Table 10. The sequence of the content in a module is given by considering the general to the specific approach.

5.5.1 Module 1: basic cyber security and Module 2: advanced cyber security

The objective of M1: Basic Cyber Security is to familiarize the crew and office staff with essential notions, cyber risks, and mitigation measures. However, Module 2: Advanced Cyber Security offers more details about cyber security. For

Table 10 Prerequisite modules

Desired module	Required module
M4 Vetting requirements	M3 Regulatory requirements
M8 Cyber security investments	M3 Regulatory requirements
	M4 Vetting requirements (if it is taken)
M10 Cyber security management	M3 Regulatory requirements
	M5 Critical deck systems
	M6 Critical engine systems
	M7 Other critical systems
	M9 Cyber security practices
	M2 Advanced cyber security (if it is taken)
	M4 Vetting requirements (if it is taken)
M11 Advanced skills	M2 Advanced cyber security
	M5 Critical deck systems
	M6 Critical engine systems
	M7 Other critical systems

instance, the term of malware is explained in the M1: Basic Cyber Security module. However, in the M2: Advanced Cyber Security module, types of malware, such as ransomware, key logger, and spyware are elaborated.

5.5.2 Module 3: regulatory requirements

The module is based on the IMO requirements and recommendations, including cyber security-related resolutions, codes, conventions, and audits. The IMO issued several circulars regarding cyber risks onboard ships. To understand such requirements and recommendations, firstly the related maritime notions should be known by participants. That's why, firstly, related notions are explained in the module, such as ISM code, ISPS Code, DOC audit, SSP, SMS, and so on.

As mentioned in Sect. 5.1, an ISM Code regulation and ISPS Code recommendation are in place regarding cyber security. Such international requirements are explained to participants in this module. Flag state requirements and recommendations may be also involved. Based on the flag state of managed vessels, the circulars could be explained to participants. Potential deficiencies in audits and best practices can be shared with attendees. For instance, the combination of the Cyber Security Assessment with SSA could be an effective best practice for companies.

5.5.3 Module 4: vetting requirements

Tankers and dry cargo vessels might be subject to vetting requirements. Vetting programmes, such as SIRE, CDI, TMSA, and RightShip, are significant for the commercial life of a company. That's why competitive companies struggle to fulfil vetting requirements, such as training, risk assessment, policy, and procedures.

The module comprises cyber security requirements in tanker and dry cargo vessel audits. SIRE, CDI, and TMSA are for tankers, but RightShip is for dry cargo vessels. A company operating only dry cargo vessels doesn't need to be familiar with the requirements of tanker vetting programmes. Moreover, each tanker operator may not be subject to all types of tanker audits. For instance, a company operating petroleum tankers may not need to be familiar with CDI requirements. Because of these reasons, the module can be specifically designed by considering attendees' learning needs.

5.5.4 Modules 5–6–7: critical deck, engine and other systems

The IMO divides the vulnerable systems onboard into eight categories, such as bridge systems, cargo handling and management systems, propulsion and machinery management and power control systems, access control systems, passenger servicing and management systems, passenger-facing public networks, administrative and crew welfare systems, and communication systems [56].

Although the IMO broke vulnerable systems onboard into eight categories, we investigated the cyber risks of such systems under three modules (i.e. Modules 5, 6, and 7) by considering the roles and responsibilities of the crew onboard. The master and deck officers are responsible for the operation of bridge systems, cargo handling and management systems, and communication systems. The engineer officers are responsible for propulsion and machinery management and power control systems. Module 7: Other Critical Systems was designed for the cyber risks of access control systems, passenger servicing and management systems, passenger-facing public networks, and administrative and crew welfare systems. Module 7 may need to be designed as ship specific. For instance, a cargo ship might not have a network for passengers.

5.5.5 Module 8: cyber security investments

Financial investments are crucial for cyber-secured systems. Investments are typically decided by management-level staff, such as the CEO, CFO, directors, or department leaders. This module is developed for key staff in a company to make an easier decision in cyber security investments. Moreover, the key staff is trained about optimum investment costs for cyber

security. Investments are not only limited to costs of technical measures (e.g. antivirus license costs). For example, flag states and class societies started to offer cyber security notations for ships. The managers may be eager to make a contract with 3rd parties for the protection, response, and recovery process. ISO 27001 information security management certification could be considered to be awarded. Last but not least, the key staff should be informed about Clause (CL) 380 in marine insurance policies (e.g. P&I and H&M) [25].

5.5.6 Module 9: cyber security practices

The module comprises hands-on training and may need to be designed company-specific. The attendee can learn the use of physical security tools (e.g. USB port lockers) and software security tools (e.g. antivirus and password management software). The update of the operating system and antivirus software are demonstrated. Furthermore, internet protocols onboard, such as Fleet Broadband (FBB), Very Small Aperture Terminal (VSAT), or mobile connections (e.g. 4 G and 5 G) are explained to make understand the cost and speed differences between connection types. Cyber security plans and procedures of the company can be explained to attendees. A risk assessment may be performed for potential cyber risks, as well. The attendee can learn how to be filled out the company documents, such as the checklist to follow in case of a cyber attack or the physical notebook to keep passwords. Last but not least, the attendee learns how to give effective training in this module.

5.5.7 Module 10: cyber security management

The module is designed for cyber security managers in companies. The participants learn to develop procedures, including protection, detection, response and recovery plans for cyber security. Participants will be also familiar with potential mutual points between maritime and cyber security, such as management of change procedures, internal audits onboard and office, ship-shore combined drills, and risk management. They learn the points that should be considered in alteration and new building projects. In this module, useful materials, including checklists, posters, guidelines, books, and such are introduced to participants, as well.

5.5.8 Module 11: advanced skills

In this module, the participants learn advanced cyber security tools, such as firewalls. They will learn system and network administration as well as penetration testing tools. Each vessel may have different risks. For instance, fishing and passenger ships don't have the same risks. Passenger ships inherently have additional risks because of the complex IT network for passenger welfare systems. That's why companies may assign a dedicated CySO to the office or vessel. Module 11 is designed particularly for dedicated cyber security staff.

5.6 Select instructional strategies

The objective of this step is to determine the appropriate instructional strategies for the curriculum identified [93]. Five instructional strategies are proposed for the modules identified, such as lecture, discussion, case study, drill, and demonstration. A module can be given with a strategy or a combination of multiple strategies.

A lecture is a one-way presentation from a speaker to participants [93]. Discussion is sharing ideas among participants about a specific topic [93]. Case studies, such as incidents, situations, stories, and scenarios are tools to develop critical thinking skills [93, 136]. A drill is a structured practice to strengthen previous learning [93]. The demonstration is a presentation and exercise about how to perform a procedure and use software or hardware [93].

The lectures in the MarCy programme can be given conventionally to learners. However modern training approaches can also be performed, such as adaptive learning [69] and flipped learning [34] techniques. The mentioned strategies, except the demonstration, can be given online, on-site (in the institutes, company offices, and seminar halls, etc.), and hybrid. The demonstration modality should be performed on-site. Hybrid training courses can be organized as multi-hub, as well. Given that the internet connection could be limited, video training courses should be also considered for ships. Drills are typically based on a structured scenario. The participants shouldn't be aware of the scenario before the drill to understand their real reactions. A ship-shore combined drill may also be performed. Table 11 represents the potential instructional strategies for each module.

5.7 Obtain instructional resources

The objective of this step is to ensure that all required resources for the training are in place. In this section, we focus on physical and human resources, and training materials. [93]

Physical resources are regarding the facility, tools, and equipment. On-site training needs a physical environment, such as an air-conditioned classroom, blackboard, projector screen, projector, and computer could be required. If the online training is live, a camera, microphone, speaker (or headset), and light may be required, as well as their spares [107]. A reliable and broadband internet is necessary [107]. Alternative internet and electricity options should be provided because of the potential risks of disruptions [107]. Marine components and simulators depending on the

Table 11 Potential instructional strategies

Code	Title	Instructional strategies				
		Lecture	Discussion	Case study	Drill	Demonstration
M1	Basic cyber security	✓	✓	✓		✓
M2	Advanced cyber security	✓	✓	✓		
M3	Regulatory requirements	✓	✓			
M4	Vetting requirements	✓	✓			
M5	Critical deck systems	✓	✓	✓	✓	✓
M6	Critical engine systems	✓	✓	✓	✓	✓
M7	Other critical systems	✓	✓	✓	✓	✓
M8	Cyber security investments	✓	✓			
M9	Cyber security practices	✓			✓	✓
M10	Cyber security management	✓	✓			
M11	Advanced skills	✓			✓	✓

design of the training can be used. Particularly Module 11: Advanced Skills needs various software and computers for the demonstration.

Lecturers should be selected studiously. Given that each module or content may require different expertise, each one can be given by a different expert. For instance, Module 4: Vetting requirements could be given by a lecturer with having maritime background. However, Module 11: Advanced Skills can be given more effectively by a lecturer coming from the cyber security field. The background of the lecturer solely is not sufficient to give such training. For instance, each professional in the maritime sector is not familiar with vetting programmes. On the other hand, professionals can be familiar with vetting programmes, but cannot be familiar with cyber security requirements in the vetting programmes. That's why the experience and knowledge of the potential lecturers should be considered while hiring.

The training materials are books, scientific papers, guidelines, circulars, animations, videos, presentations, photos, and such. Several training materials have been published by credible organizations, as mentioned in Sect. 2.2. Moreover, the Republic of the Marshall Islands Maritime Administrator published a circular, including maritime cyber risk management resources [114]. Such documents can be used as training materials in the modules. In Appendix 1, potential training materials by modules, such as books, theses, scientific papers, guidelines, and questionnaires are represented, however, the resources are not only limited to them.

5.8 Conduct training

The objective of this step is to perform the training designed. Before the training, a schedule can be identified for relaxation. During this period, drinks and snacks can be provided. If a social event is organized one day before the training, limited alcohol can be served. However, if only a limited time exists before the training, soft drinks should be served to participants. For the food, the diets of the participants should be considered. For instance, some participants could be vegan or allergic. Attendees could be tired or busy with their tasks. Managers need a substitute in particular. Otherwise, they may not attend to training programme completely.[93]

The modules can be slightly modified by considering the attendees' needs [93]. That's why attendees' needs should be understood before delivering each module or during the training. Correct training materials, more than the required number, should be ready for the participants [93]. The training can start with a short opening. If the training is recorded, the attendees should be notified in the opening. In an onsite training course, the participants should be informed about safety instructions in case of an emergency situation. Attendees should know the agenda and the objectives of the training and modules. Moreover, requirements for the completion of the training should be explained in the opening speech, such as a potential exam at the end of the training. The training schedule should be followed as far as possible. The training should be summarized in the conclusion. The last questions of the participants can be addressed.

The duration of the modules can be identified by considering the learning needs of the participants and the decisions of the responsible managers in a company. The contents of a module can be extended or narrowed by considering reserving time for the training. On the other hand, instructional strategies could be decreased or increased. For instance, a module can be given as only a lecture instead of a combination of lecture and case study to decrease the training period. The recommended training duration by modules is represented in Table 12. Such suggestions for the training period don't include the required time for the examination. Some modules (e.g. Module 1: Basic Cyber Security) can be given onboard. In such a case, training may need to be short. The recommended training duration of Module 9: Cyber Secu-

Table 12 Recommended training duration by modules

Module	Recommended training duration
each module from Module 1 to Module 8	2 h
Module 9: Cyber Security Practices	8 h (1 day)
Module 10: Cyber Security Management	40 h (5 days)
Module 11: Advanced Skills	depends on the participant's background

rity Practices and Module 10: Cyber Security Management are affected from the specialized curriculum, including software and procedural demonstration. Module 11: Advanced Skills depends on the participant's background but would be a long-term module. Such training modules may need to be repeated at least once a year.

5.9 Evaluation and feedback

The evaluation phase is to examine the outcomes and objectives of the training designed. According to the recommendations provided in the CEM, training evaluation should occur two-fold: (1) continuous (formative) evaluation of training components developed should occur during the design of a training course and (2) summative assessment should occur at the conclusion of training [93].

The first type of evaluation would allow to analyse and revise each component developed of the training programme before conducting training. The main advantage of evaluating at this stage is ensuring that training is aligned with participants' needs, as mentioned in [22]. Such form of evaluation and revision should occur throughout the life cycle of development, whenever key components are selected or developed in the previous steps of the programme. The main advantage of conducting continuous evaluation is that it helps in targeting precise components that may need revision instead of having to re-assess the whole training course.

Summative assessment or post-training tests, on the other hand, would allow for both evaluations of the performance of training participants post-training, as well as feedback collection. During the discussions conducted in the Delphi method used to evaluate the MarCy programme, participants suggested a number of qualitative and quantitative approaches to conduct this type of assessment, including using performance indicators and metrics, ranging from multiple-choice exams to log and system analysis for computer-based training. When it comes to qualitative evaluation, recommendations included discussion-based or survey-based feedback collection, observation and post-evaluation from external, senior personnel.

The data collected by the formative and summative assessments are critical for improving and revising the training offerings developed using the MarCy programme in successive iterations. Moreover, they can also provide a measure to improve the programme itself.

In addition to formative and summative evaluation, CEM recommendations include utilizing pre-tests. These tests should be administered before training is conducted and serve as knowledge and competence pre-assessment of the participants.

6 Evaluation of the programme

As previously discussed in Sect. 4, the evaluation of the MarCy programme was conducted using the Delphi method across two rounds. In both rounds, participants engaged in discussions concerning various aspects of maritime cyber security training and provided feedback on the MarCy programme. A comprehensive summary of the outcomes from the discussions during each round of the Delphi process is presented in the subsequent sections.

6.1 Main considerations that distinguish maritime cyber security training from other cyber security disciplines

In the context of maritime cyber security training, the unique operating environment of the maritime industry presents distinctive challenges compared to other sectors. Vessels face a range of complexities that demand specialized training approaches. One notable consideration is the potential difficulty in responding to a cyber attack promptly. Unlike land-based organizations, accessing a vessel for immediate response by a cyber security expert may prove challenging due to its remote location and limited connectivity to the internet. Moreover, the dynamic nature of maritime operations adds another layer of complexity. During a cyber attack, a vessel may be sailing, and the consequences of an attack, especially those affecting critical navigation systems, could lead to marine incidents such as collisions. Therefore, seafarers should be trained to recognize and respond to cyber threats. Furthermore, training programmes should be designed by considering the unique systems onboard, vetting and regulatory compliance, and the various roles and responsibilities of crew members.

6.2 Recommended training methods for maritime cyber security

Participants have given various recommendations, ranging from simulation-based approaches to classroom training. The main advantage of simulation-based training is allowing

for hands-on training based on realistic scenarios, without causing security risks to vessels. A downside mentioned of simulation-based training was relative to implementation costs. To solve this issue, Virtual Reality (VR) based simulation training was recommended to be further developed. Classroom training was instead recommended due to a preference for face-to-face training. This was highlighted as many of the current Computer-based Training (CBT) solutions were seen to be ineffective at engaging participants. Overall, it was recommended to combine simulation-based and classroom-based training when possible, and keep a focus on real-life scenarios.

6.3 Limitations of current offerings in maritime cyber security training

Several limitations were highlighted by participants regarding current maritime cyber security training. These included lack of IT background of seafarers, limited material available for maritime cyber security training, lack of resources (e.g. time, fatigue, and onboard broadband internet) to conduct onboard training, lack of the IMO requirements for maritime cyber security training and of qualified trainers, budget limitations, heterogeneous systems between different vessels, lack of targeted training, need for language considerations in training provision, lack of motivation to pursue higher cyber security competences, and finally lack of cyber-threat intelligence sharing.

6.4 Solutions to current limitations

To resolve the limitations previously mentioned, participants suggested several measures, including; focusing on real-life case studies and scenarios to engage participants; updating training regularly; mandating training to new employees and ensuring it is repeated or continued for existing employees; adapting training to different languages; adding maritime cyber security training to formal education of cadets, encourage information sharing between different companies; promoting maritime cyber security training and cyber security culture using a top-down approach, with senior management championing these; use a bottom-up approach to ensure that all training elements are tied to relevant cyber security components; lecturers' expertise should be considered other than their academic titles or the companies/institutes they work for.

6.5 Methods & criteria for evaluating maritime cyber security training

Evaluation of training was noted to be often less prioritized or sidestepped. This has been considered a key challenge in maritime cyber security training, as it limits training effectiveness and improvement. Recommended methods from participants consisted of a combination of qualitative and quantitative approaches. When it comes to quantitative approaches, participants suggested using performance indicators and metrics, ranging from multiple-choice exams to log and system analysis, in the case of CBT and simulation training. When it comes to qualitative evaluation, recommendations included discussion-based or survey-based feedback collection, observation and post-evaluation from external, senior personnel. Overall, it was agreed that evaluation should be defined based on the type and content of the training.

6.6 Additional considerations/comments

Participants followed the discussion with personal considerations about additional recommendations and considerations for maritime cyber security training. One consideration was introducing a new role: a dedicated CySO for either onboard (i.e. SCySO) or off-board duty (i.e. CCySO). This would be particularly valuable for larger size companies. Another point of discussion raised by participants focused on the real-life effectiveness of training. As cyber security training is becoming more commonplace and standardized, there is often an assumption that a company is sufficiently secure once training is completed. This may not reflect the actual state of preparedness of employees, as certifications obtained post-training often do not guarantee proper cyber security.

6.7 Feedback on the MarCy programme

When it comes to the evaluation of the MarCy programme, the majority of the participants found it to be well-structured and comprehensive. That being said, a number of recommendations for improvements were reflected to the programme. Table 13 summarizes all recommendations made during the multiple rounds of Delphi.

7 Discussion

The MarCy programme is an effective tool for instructional designers in designing maritime cyber security training programmes. The recommendations were developed not solely based on the authors' opinions but also with contributions from experts in the field. In other words, the MarCy is a programme agreed upon by multiple experts. To the best of our knowledge, this aspect is unique in the literature.

After designing the MarCy programme, we gathered expert opinions using the Delphi technique. The presence of authors working in maritime cyber security facilitated finding experts, allowing contributions from a diverse range of companies and institutions spanning from the USA to Singapore. Following the CEM approach would have required at least

Table 13 Summary of recommendations for the MarCy programme

Topic	Recommendation
Roles Identification	The Board of Directors in the company organization chart should not include the CEO. The Board of Directors should be separated
Training Modules	Titles of modules M5 Vulnerable Deck Systems, M6 Vulnerable Engine Systems, M7 Other Vulnerable Systems, should be replaced vulnerable with critical. A process should be offered for the module selection
Learning Outcomes	Some of the contents of M10 Cyber Security Management module could be introduced in the M1 Basic Cyber Security module, with lessened complexity
Modules' Prerequisites	Modules of M5 Vulnerable Deck Systems, M6 Vulnerable Engine System, and M7 Other Vulnerable System should be required before the M11 Advanced Skills module
Learning needs	M1 Basic Cyber Security module should include the consequences of cyber attacks. M10 Cyber Security Management module should include best practices. Differences between various standards and frameworks should be discussed (e.g. ISA/IEC 62443 Series of Standards)
Training Requirements Comprehensiveness	Some types of ships, such as passenger ships, need fully dedicated Cyber Security Officers. Such a role may need longer and more detailed training, such as a master's degree
Considerations for Educators	Qualified lecturers for maritime cyber security training are difficult to find. Thus, contents can be given by different lecturers
Education and Training Cycle	Periodical re-training should occur at least once a year. Training follow-ups should occur at a higher frequency (e.g. once or twice a year, depending on requirements)
Additional Comments	The curriculum for onboard training could be too long. Training should be either given only at the shore or the training curriculum should be reduced, and/or several instructional strategies (e.g. case study and discussion) should be removed to shorten the training time. M10 Cyber Security Management module is designed for the roles managing cyber security matters in the company. However, the module should be also taken by top management of the company. Not only occurred but also potential cyber incidents should be included in training needs

eight meetings, which, considering time zone differences, might have reduced participation. We observed that the Delphi method could be used to validate similar programmes like MarCy, especially in fields with limited experts for designing specialized training.

Although the MarCy programme has not been implemented in a real training session, real-world applications are in place in the literature. We also intend to organize training sessions with various learner groups in the maritime sector to evaluate all stages of the MarCy programme and present our findings in an additional study.

It would be beneficial to implement the MarCy programme by two distinct groups. One group consists of the authors who proposed the programme, while the other includes instructional designers beyond the authors who can also test the MarCy programme. These designers could come from diverse backgrounds, including maritime and cyber security. This approach would yield varied findings.

While the MarCy programme is customized for maritime purposes, its modular approach can be used to develop a wide range of training programmes. It is not limited to maritime contexts or cyber security training alone. It can also be applied to designing formal education beyond industry-specific training.

In our study, we defined the application domain as cyber security training for both office and maritime personnel in maritime companies. The existing modules will address the training needs of many maritime professionals, but additional modules might be necessary. For instance, individuals working in shore control centres during the remote operation of autonomous ships might require a module specific to autonomous vessels. Navy personnel might need training against cyber attacks targeting military systems like fire control systems on warships. Workers in container terminals might need to learn about specific cyber risks related to container tracking systems.

The curriculum in the MarCy programme is provided in broad strokes and not overly detailed. For example, naval ships may have components like War (W)-AIS and W-ECDIS developed for military purposes. Therefore, curriculum preparation needs to consider the participant profile.

We believe that the MarCy programme will significantly facilitate the design of cyber security training for maritime sector stakeholders. Nonetheless, we still consider expert involvement in designing training to be highly valuable. As mentioned in Sect. 5.7, the training should be ideally delivered by experts. Given the scarcity of experts in the maritime cyber security field, dividing the curriculum and having

different experts teach based on their specialities could be beneficial.

As previously mentioned, maritime cyber security training is offered by various institutions and is documented in the literature. However, openly accessible curriculums are limited. The MarCy programme provides comprehensive curriculum suggestions for instructional designers. Even if a designer chooses not to use the MarCy programme, the provided curriculum can still be valuable.

While this study does not primarily aim to conduct a literature review on maritime cyber security training, it encompasses a thorough examination of existing training, recommendations from academic publications, considerations in vetting programmes and class notations. Thus, it provides a broad perspective to readers and guides researchers to areas requiring further investigation. Furthermore, readers unfamiliar with the maritime sector gain basic insights into the organizational structure and responsibilities within ships and offices.

Through this work, we extend the CEM and contribute scientifically to the literature while facilitating the design of maritime cyber security training for industry experts. In other words, we believe that our study not only holds scientific value but also addresses the practical needs of the maritime sector.

8 Conclusions

In conclusion, the mounting concern surrounding cyber risks within the maritime industry has necessitated a call for swift, proactive measures. The potential fallout from a successful cyber attack—including economic losses, data breaches, and compromised operational safety—underscores the utmost importance of cyber awareness. Training emerges as an indispensable tool to heighten cyber awareness and subsequently shield against these threats. This need has garnered support, finding its place within vetting programmes, cyber notations of class societies and flag states, and even proposed integration within the STCW for seafarers.

The distinct responsibilities and roles held by employees necessitate customized training methodologies. In response, we proposed the MarCy training programme by implementing the CEM to address the unique demands of professionals in maritime cyber security training. This transformation commenced by distilling a modular training programme from the CEM. Due to the scarcity of maritime cyber security experts on a global scale and the CEM's mandate for a minimum of eight meetings with experts, the evaluation phase underwent meticulous adjustments. Last, all stages are customized for maritime cyber security training. The MarCy training programme, born from the tenets of the CEM, encompasses a meticulous nine-stage process:

1. identify the needs of the organization;
2. specify job performance;
3. identify learner needs;
4. determine objectives;
5. build curriculum;
6. select instructional strategies;
7. obtain instructional resources;
8. conduct training;
9. evaluation and feedback.

By implementing the MarCy programme, we have defined eleven elective training modules specifically designed to enhance the knowledge, skills, and attitudes of seafarers and office personnel in safeguarding against maritime cyber risks. Additionally, the programme's flexibility enables it to be tailored to meet the diverse needs of various stakeholders within the maritime domain. The training modules proposed in this study include:

- M1: Basic cyber security;
- M2: Advanced cyber security;
- M3: Regulatory requirements;
- M4: Vetting requirements;
- M5: Critical deck systems;
- M6: Critical engine systems;
- M7: Other critical systems;
- M8: Cyber security investments;
- M9: Cyber security practices;
- M10: Cyber security management;
- M11: Advanced skills.

The carefully selected modules were aligned with the potential responsibilities within a company's organizational structure. Onboard positions like Master and Chief Engineer, as well as office roles such as CEO, CFO, DPA, and more, were thoroughly considered. Subsequently, we outlined the objectives and curriculum for each training module. Instructional strategies, such as lectures, discussions, case studies, drills, and demonstrations, were carefully recommended for each module. Additionally, we paid close attention to the required physical and human resources, as well as the necessary training materials. Finally, we delved into determining the optimal duration for each module, while also addressing key considerations for the training sessions.

The robustness of the MarCy programme was subsequently confirmed through a Delphi technique involving 19 experts from both academic and industrial backgrounds, resulting in refinements based on their insights. During the Delphi rounds, discussions also revolved around the multifaceted dimensions of maritime cyber security training. Novel strategies, such as VR-based simulations were proposed as innovative instructional solutions. Furthermore, the

vital role of comprehensive evaluation methods for learners, encompassing both qualitative and quantitative dimensions, was strongly emphasized. Given the limited availability of publicly accessible information on past cyber incidents, it was noted that stakeholders should be encouraged to provide detailed information about occurred incidents. To enhance effective countermeasures, the proposal was made to assign dedicated cyber security roles, especially within larger shipping companies.

The potential of the MarCy programme is not confined to its current scope. It boasts the adaptability to embrace additional modules, catering to a diverse array of learner groups and scenarios. From professionals in port facilities to those in the shore control centres of autonomous vessels, and even within governmental entities like maritime administrations and naval forces, the programme's application is far-reaching. Furthermore, it extends its utility to crafting formal education courses. Our forthcoming endeavours are geared towards the deployment of this programme across diverse learner groups within the maritime domain, fostering a well-informed and resilient maritime cyber security community.

Acknowledgements We would like to express our sincere gratitude to experts, particularly Ahmed Amro, for their comments towards improving our study.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital).

Research Data Policy and Data Availability Statements: Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Funding: This paper has received funding from the Research Council of Norway through the Maritime Cyber Resilience (MarCy, project number 295077) project. The content reflects only the authors' views, and neither the Research Council of Norway nor the project partners are responsible for any use that may be made of the information it contains.

Conflicts of Interest: The author declares no conflict of interest.

A Appendix

The proposed curriculum and potential training materials for the modules are provided below, along with the corresponding starting page numbers of sections from the books, guidelines, and questionnaires. *E* depicts essential contents and *H* represents helpful contents in the table. Both of these are explained in Sect. 5.5. *Specific* means the training material should be prepared company-specific, such as checklists in the SMS of a company. On the other hand, *not found* expresses a useful training material for the content is not found (Table 14).

Table 14 Curriculum and potential materials by training modules

Content	E/H	Material
M1 Basic Cyber Security		
Definitions	E	[14, p.58], [47, p.7], [139, p.xi], [63, p.5]
Importance of cyber security for ships	H	[47, p.19]
Typical vulnerable systems onboard	E	[14, p.48], [139, p.5]
Common vulnerabilities	E	[14, p.17]
Cyber incidents in the maritime industry	E	[14, pp.10,11,18,21,32,36], [70, p.69]
Signs and consequences of a cyber incidents	E	[139, p.33]
Ship to shore interface and remote access	E	[14, p.19]; [139, p.101]
Ship visits	E	[14, p.20]
Creating secure password	E	[139, p.16], [8, p.5]
Port security (e.g. USB and RJ-45)	E	[139, p.41]
Wifi security	E	[139, p.50]
Social engineering	E	[139, p.9], [70, p.33]
Phishing	E	[8, p.7], [139, p.9], [70, p.35]
M2 advanced cyber security		
Threat actors and their motivations	E	[14, p.12] , [47, p.34] , [139, p.7]
IT / OT systems and differences	E	[14, p.7], [139, p.61]
Stages of a cyber incident	E	[14, p.14]
Types of cyber threats	E	[14, p.13], [139, p.8], [70, p.32]
Types of malware (e.g. key logger, and ransomware)	E	[139, p.8]
M3 regulatory requirements		
Maritime notions (e.g. ISM Code, ISPS Code, SSP, SMS, DOC audit)	H	[53, 54, 139]
ISM Code requirements, potential deficiencies, and best practices	E	[139, pp.1,32,151], [59]
ISPS Code recommendations and best practices	E	[139, pp.1,151], [50]
Flag state circulars, regional regulations, potential deficiencies, and best practices	E	[47, p.14], [139, p.1,32,151], [137]
Forthcoming regulations	H	[51]
M4 Vetting Requirements		
Vetting programmes and their impact on the business life of a company	H	[106]
SIRE requirements, potential deficiencies, and best practices	E	[106], [100, p.74]
SIRE 2.0 requirements, potential deficiencies, and best practices	E	[101, p.707]
CDI requirements, potential deficiencies, and best practices	E	[106], [21, p.151]
TMSA requirements, potential deficiencies, and best practices	E	[106], [102, p.104]
RightShip requirements, potential deficiencies, and best practices	E	[115, p.162]
M5 critical deck systems		
Target deck systems (bridge systems, cargo handling and management systems, communication systems)	E	[14, p.48], [47, p.38], [139, p.75], [70, p.117]
Threats and vulnerabilities	E	[65, pp.20,23,25]
Mitigation measures	E	[65, pp.28,30,33], [139]
Redundant systems	E	Not found
Incident response	E	[139, p.45]

Table 14 continued

Content	E/H	Material
M6 critical engine systems		
Target engine systems (propulsion and machinery management and power control systems)	E	[14, p.48], [47, p.39], [139, p.75], [70, p.118]
Threats and vulnerabilities	E	[65, p.22]
Mitigation measures	E	[65, p.30]
Redundant systems	E	Not found
Incident response	E	[139, p.45]
M7 other critical systems		
Other vulnerable systems (access control systems, passenger servicing and management systems, passenger-facing public networks, administrative and crew welfare systems)	E	[14, p.49], [47, p.39], [139, p.75], [70, p.123]
Threats and vulnerabilities	E	Not found
Mitigation measures	E	Not found
Redundant systems	E	Not found
Incident response	E	[139, p.45]
M8 cyber security investments		
Importance of senior management involvement	E	[14, p.6]
Contract/consultancy with third parties (e.g. for training, maintenance, incident response)	E	[139, p.51]
ISO certifications (e.g. ISO 27000)	E	[64]
cyber security class & flag notations	E	[2, 29, 63, 91]
Marine insurance policies (e.g. P&I and H&M)	H	[25]
Clause (CL) 380 in marine insurance policies	E	[25]
Decision-making on optimum investment cost	E	[67]
New building and alteration projects	E	[139, p.87]
M9 cyber security practices		
Role of CySO	E	[47, p.27], [139, p.91]
Ethical considerations of maritime cyber security	E	[105]
Performing checklists, policies, and procedures	E	Specific
Training of onboard trainers	E	Not found
Internet protocols onboard (e.g. VSAT, FBB, 4G, and 5G)	H	Not found
Software update (e.g. ECDIS)	E	[139, p.80]
Operating system update (e.g. Windows)	E	[139, p.20]
Antivirus update (e.g. ESET Endpoint Security)	E	[139, p.24]
Use of cyber security tools (e.g. antivirus software and USB lockers)	E	specific
M10 cyber security management		
Developing a cyber security plan and cyber security assessment	E	[47, pp.23,49], [139, pp.30,96,149], [63, p.12]
Roles and responsibilities	E	[14, p.7], [139, pp.93,95]
Protection measures	E	[14, p.30], [47, p.51], [139, p.17], [8, p.17], [23, p.10]
Detection methods	E	[14, p.40], [139, p.45]
Response procedures	E	[14, p.43], [139, p.45]
Recovery procedures	E	[14, p.45], [139, p.45]
Cyber incident follow-up	E	Not found
Asset management	E	[139, p.107], [63, pp.15,22,30,43]
Risk assessment & management	E	[14, p.26], [70, p.188]

Table 14 continued

Content	E/H	Material
Password management	E	[139, p.16]
Communication and relationship with third parties (e.g. vendors and agents)	E	[14, p.9,20], [47, pp.30,57]
Mutual points between cyber security and maritime (e.g. Change Management)	H	Not found
Standards and frameworks (e.g. ISA/IEC 62443, IEC 63154, and MITRE ATT&CK)	E	[45, 46, 89]
Designing a training programme	E	[14, p.34], [139, p.31]
Cyber security drills (e.g. ship-shore combined drill)	E	[139, p.39]
Useful materials (e.g. checklists, posters, guidelines and books)	H	[14, 47, 70, 139]
M11 advanced skills		
System administration	E	[78]
Network administration	E	[78]
Use of penetration testing tools	E	[122]
use of advanced cyber security tools (e.g. firewall)	E	specific

B. Appendix

The essential questions asked regarding maritime cyber security and the MarCy programme are below. However, the discussions in Delphi rounds were not limited to only such questions.

The essential questions for maritime cyber security:

- In your opinion, what are the main considerations that distinguish maritime cyber security training to other cyber security disciplines?
- In your opinion, what are the best training methods for maritime cyber security?
- In your opinion, what are the main limitations of current offerings in maritime cyber security training?
- How would you address these limitations?
- How do you think maritime cyber security training should be evaluated?
- Are there additional considerations/comments you would like to share?

The essential questions for the training programme:

- Do you think the verification with the Delphi technique is appropriate for developing a maritime cyber security training programme? If not, please motivate.
- Are the training needs addressed completely in the programme? If not, please advise other requirements or recommendations.
- Can the training requirements of a company be accomplished with this training programme?
- Are the individual roles of the crew and office staff identified correctly?
- Are the training modules identified by the programme sufficient and comprehensive? If not, please motivate.
- Are the module objectives acceptable?
- Do the learning outcomes meet the module objectives correctly?
- Is the proposed process for the module selection convenient?
- Are the prerequisites listed in the correct order?
- Does the curriculum meet module objectives?
- Does the curriculum meet the needs of roles identified against the cyber risks?
- Does the curriculum meet the learning needs of a company?
- Are the instructional strategies convenient for the curriculum?
- Can qualified lecturers be provided for training modules?
- Does the training need to be repeated?
- Are there additional considerations/comments you would like to share?

References

1. Aboamare. Maritime cyber security introduction course. 2022. https://www.aboamare.fi/maritimecyber-security (visited on 09/28/2022)
2. ABS. Guide for cybersecurity implementation for the marine and offshore industries. Texas, USA, 2021. https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/251_cybersafety_2021/cybersafety-v2-cybersecurity-guide-feb21.pdf (visited on 09/15/2022)
3. Adams, N.P.H. et al.: How port security has to evolve to address the cyber-physical security threat: lessons from the SAURON project.

In: International Journal of Transport Development and Integration 4.1 (2020), pp. 29–41
4. Ahvenjarvi, S., Czarnowski, I., Mogensen, J.: Addressing Cyber Security in Maritime Education and Training (CYMET). Ed. by Gamal Ahmed Mohamed Ghalwash and Aykut Olcer. Tokyo, Japan, 2019. http://archive.iamu-edu.org/download/final-report-of-research-project-fy2018/?wpdmdl=6691 (visited on 09/29/2022)
5. Akpan, F., et al.: Cybersecurity challenges in the maritime sector. Network 2.1 (2022). https://doi.org/10.3390/network2010009
6. Amundsen, T., Skar, B., Slinning, I.: K16 Textbook maritime English. Engine officer: Chapter 4: My workplace. ISBN: 978-82-93766-18-6. https://www.marfag.no/k16/kap-4 (visited on 09/20/2022)
7. Androjna, A., Satler, T.B., Srše, J.: An Overview of Maritime Cyber Security Challenges. In: 19th International Conference on Transport Science. 2020
8. ANSSI. Best practices for cyber security on board ships. 2016. https://www.ssi.gouv.fr/uploads/2017/06/best-practices-for-cyber-security-on-board-ships_anssi.pdf (visited on 02/06/2023)
9. Aris et al.: Multidisciplinary curriculum design approaches towards balanced and holistic graduates. In: 2017 IEEE 9th International Conference on Engineering Education (ICEED). IEEE, 2017
10. Bacasdoon et al.: A multiple case study of METI cybersecurity education and training: A basis for the development of a guiding framework for educational approaches. In: TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation 16.2 (2022), pp. 319–334. https://doi.org/10.12716/1001.16.02.15
11. BCA College.: MSc Maritime Cyber Security. https://www.bca.edu.gr/en/master-degrees/shipping-transport-logistics-department/msc-maritime-cybersecurity/ (visited on 11/04/2022)
12. Bhattacharjee, S.: A guide to merchant navy ranks. 2020. https://www.marineinsight.com/careers-2/a-guide-to-merchant-navy-officer-ranks/ (visited on 09/20/2022)
13. BIMCO and ICS.: Seafarer workforce report. Scotland, UK, 2021. https://shop.witherbys.com/seafarer-workforce-report/ (visited on 10/06/2022)
14. BIMCO et al.: The guidelines on cyber security onboard ships. 2020. https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf (visited on 03/21/2022)
15. Blenkey, N.: ABS issues first Cyber Security-Ready notation to HHI VLCC. 2018. https://www.marinelog.com/news/abs-issues-first-cyber-security-ready-notation-to-hhi-vlcc/ (visited on 07/30/2022)
16. Bobbitt, F.: Scientific method in curriculum-making. In: Flinders, D.J., Thornton, S.J. (eds.) The curriculum studies reader, pp. 15–21. Routledge, New York, USA (2009)
17. Cambridge. Attitude. https://dictionary.cambridge.org/dictionary/english/attitude (visited on 11/06/2022)
18. Richaurd, R., Camp, P., Blanchard, N., Gregory, E.: Huszczo. Toward a more organizationally effective training strategy & practice. New Jersey and USA: Prentice-Hall, 1986
19. CBS. Maritime cyber security and big data. 2017. https://cbs-executive.dk/wp-content/uploads/2017/06/Maritime-Cyber-Security-Big-Data-2017.pdf (visited on 09/28/2022)
20. CBS. Maritime cyber security for managers. https://cbs-executive.dk/wp-content/uploads/2017/06/Maritime-Cyber-Security.pdf (visited on 09/28/2022)
21. CDI. Ship Inspection Report Chemical Tanker. 2019. https://www.cdim.org/webshop/cdi/fr_cdim.jsp (visited on 10/25/2022)
22. Chowdhury, N., Katsikas, S., Gkioulos, V.: Modeling effective cybersecurity training frameworks: a delphi method-based study. Comput. Secur. **113**, 102551 (2022). https://doi.org/10.1016/j.cose.2021.102551
23. Class, N.K.: Guidelines for designing cyber security onboard ships. Tokyo, Japan, 2020. https://www.nextdeal.gr/sites/default/files/sitefiles_2020-07/guidelines_for_designing_cyber_security_onboard_ships.pdf (visited on 10/23/2022)
24. Coskun Yasar, G., Aslan, B.: Curriculum theory: a review study. Int. J. Curric. Instr. Stud. **112**, 237–260 (2021). https://doi.org/10.31704/ijocis.2021.012.
25. Dadiani, D.: Cyber-security and marine insurance. MSc. Malmö, Sweden: World Maritime University, 2018. https://commons.wmu.se/cgi/viewcontent.cgi?article=1606&context=all_dissertations (visited on 10/15/2022)
26. Digital Ship.: KR issues first cybersecurity class notation to HHI for very large LPG carriers. 2020. https://thedigitalship.com/news/maritime-satellite-communications/item/6801-krissues-first-cybersecurity-class-notation-to-hhi-for-very-large-lpg-carriers (visited on 07/30/2022)
27. Dilnoza, M., et al.: Modular training system as a factor of improving educational process. Int. J. Innov. Technol. Explor. Eng. **9.1**, 3160–3166 (2019)
28. DNV.: Cybersecurity given priority in TMSA 3. 2022. https://www.dnv.com/expert-story/maritime-impact/Cybersecurity-given-priority-in-TSMA3.html (visited on 11/12/2022)
29. DNV. DNV-CG-0325 Cyber secure. 2021. https://rules.dnv.com/ (visited on 10/23/2022)
30. DNV. Maritime cyber security awareness e-learning. 2022. https://www.dnv.com/maritime/maritime-academy/cyber-security-elearning.html (visited on 09/28/2022)
31. DNV. Stena Drilling and DNV GL sign contract for first Cyber Secure class notation. 2019. https://www.dnv.com/news/stena-drilling-and-dnv-gl-sign-contract-for-first-cyber-secureclass-notation-149153 (visited on 07/30/2022)
32. DSCA. Implementation guide for cyber security on vessels. 2020. https://dcsa.org/wp-content/uploads/2020/03/DCSA-Implementation-Guideline-for-BIMCO-Compliant-Cyber-Securityon-Vessels-v1.0.pdf (visited on 10/22/2022)
33. Du Plessis, A.: The importance of training and education for New Zealand entrepreneurs: some empirical evidence. J. Commun. Posit. Pract. **162**, 18–38 (2016)
34. El Miedany, Y., El Miedany, Y.: Flipped learning. In: Rheumatology Teaching: The Art and Science of Medical Education (2019), pp. 285–303
35. ENSM. Specialized Master's Degree - Cybersecurity for Maritime and Port Systems. https://www.supmaritime.fr/en/specialized-master-degree-cybersecurity-maritime-and-portsystems/ (visited on 11/04/2022)
36. Erasmus, B.: van Dyk, Piet: Training management in South Africa, 2nd edn. Oxford University Press, Cape Town, South Africa (1999)
37. Fitton, O. et al." The future of maritime cyber security. Lancaster University, 2015. http://www.research.lancs.ac.uk/portal/en/publications/the-future-of-maritime-cyber-security(d6a02f20-3125-4337-b189-e8420ca71316)/export.html (visited on 10/26/2022)
38. French, S.: The benefits and challenges of modular higher education curricula. Issues Ideas Paper **201**, 1–12 (2015)
39. Furnival, D., Crispe, J.: Technical operations management. In: Shipping operations management. Ed. by I. D. Visvikis and P. M. Panayides. Vol. 4. WMU Studies in Maritime Affairs. Cham: Springer, 2017, pp. 99–128. ISBN: 978-3-319-62364-1. https://doi.org/10.1007/978-3-319-62365-8.
40. Gaitantzi., V.P.K.: The role of different departments in a shipping company. PhD thesis. Nea Michaniona, Greece: Merchant Marine Academy of Macedonia, 2018. https://maredu.hcg.gr/modules/document/file.php/MAK265/Dissertations%20in%20English/The%20role%20of%20different%20departments%20in%20a%20shipping%20company.pdf (visited on 09/20/2022)

41. GCHQ. Government Communications Headquarters. https://www.gchq.gov.uk/ (visited on 07/21/2023)
42. Gosper, M., Ifenthaler, D. (eds.): Curriculum models for the 21st century: Using learning technologies in higher education. Springer, New York (2014)
43. GOV.UK. Maritime and Coastguard Agency. https://www.gov.uk/government/organisations/maritime-and-coastguard-agency (visited on 07/21/2023)
44. Hopcraft, R.: Developing maritime digital competencies. IEEE Commun. Stand. Mag. **5.3**, 12–18 (2021). https://doi.org/10.1109/MCOMSTD.101.2000073
45. IEC. IEC 62443 series. Geneva, Switzerland, 2009
46. IEC. IEC 63154 Maritime navigation and radiocommunication equipment and systems: Cybersecurity - General requirements, methods of testing and required test results. Geneva, Switzerland, 2021
47. IET. Code of practice: Cyber security for ships. London, UK, 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cybersecurity-code-of-practice-for-ships.pdf (visited on 09/15/2022)
48. IMO. Casualty Investigation Code. London, UK, 2008
49. IMO. FAL 39/7 Ensuring security in and facilitating international trade. Measuring toward enhancing maritime cybersecurity. London, UK, 2014
50. IMO. Guide to maritime security and the ISPS Code. London, UK, 2021
51. IMO. HTW 8/15/1 Any other business. Necessity of developing relevant provisions concerning cybersecurityrelated training for seafarers. London, UK, 2021
52. IMO. International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978. 2019. https://www.imo.org/en/OurWork/HumanElement/Pages/STCW-Convention.aspx (visited on 07/20/2023)
53. IMO. ISM Code. London, UK, 2018
54. IMO. ISPS Code. London, UK, 2002
55. IMO. MSC 98/5/2 Measures to enhance maritime security. The incorporation of cyber risk management in Safety Management Systems. London, UK, 2017
56. IMO. MSC-FAL.1-Circ.3-Rev.2 Guidelines on maritime cyber risk management. London, UK, 2022
57. IMO. MSC.1/Circ.1639 The guidelines on cyber security onboard ships. London, UK, 2021
58. IMO. Resolution A.1056(27) Promotion as widely as possible of the application of the 2006 Guidelines on fair treatment of seafarers in the event of a maritime accident. London, UK, 2011
59. IMO. Resolution MSC.428(98) Maritime cyber risk management in Safety Management Systems. London, UK, 2017
60. IMO. STCW Convention. London, UK, 2010
61. Inmarsat. Beyond compliance - Cyber risk management after 2021. 2022. https://www.inmarsat.com/en/insights/maritime/2022/beyond-compliance.html (visited on 10/25/2022)
62. IRClass. Cyber security internal auditor course. 2022. https://staging.irclass.net/academy/segment/maritime-management-system/cyber-security-internal-auditor-course/?date=08/08/2022 (visited on 10/22/2022)
63. IRClass. Guidelines on maritime cyber safety. 2018. https://www.irclass.org/media/4152/guidelines-on-maritime-cyber-safety-rev2.pdf (visited on 09/15/2022)
64. ISO/IEC. ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary. Geneva, Switzerland, 2018. https://www.iso.org/standard/73906.html (visited on 07/12/2022)
65. iTrust. Guidelines for cyber risk management in shipboard operational technology systems. 2022. https://itrust.sutd.edu.sg/news-events/news/guidelines-for-cyber-risk-management-inshipboard-ot-systems/ (visited on 04/06/2022)
66. Olivier Jacq et al. The Cyber-MAR Project: First results and perspectives on the use of hybrid cyber ranges for port cyber risk assessment. In: 2021 IEEE International Conference on Cyber Security and Resilience (CSR). 2021, pp. 409–414. DOI: https://doi.org/10.1109/CSR51186.2021.9527968.
67. Jonkeren, O., Giannopoulos, G.: Analysing critical infrastructure failure with a resilience inoperability input-output model. Econ. Syst. Res. **2.61**, 39–59 (2014)
68. Karlog. Financial department. 2016. https://www.karlog.gr/departments/financial-department (visited on 09/19/2022)
69. Kerr, P.: Adaptive learning. Elt J. **70**(1), 88–93 (2016)
70. Gary, C.K., Shepard, S.D.: Maritime cybersecurity: A guide for leaders and managers. 2nd ed. 2022
71. KR. KR cyber security awareness training. 2022. https://www.krs.co.kr/eng/Content/CF_View.aspx?MRID=431&URID=424 (visited on 09/28/2022)
72. KR. Maritime cyber security course. 2019. https://edu.orangecq.com/ (visited on 09/28/2022)
73. Kristen, K., Salih, B., Siraj, A.S.: COVID-19 digitization in maritime: understanding cyber risks. WMU J. Marit. Aff. **20.2**, 193–214 (2021)
74. Laurillard, D.: An approach to curriculum design. 2010. https://www.academia.edu/35192268/An_Approach_to_Curriculum_Design (visited on 11/01/2022)
75. Lee, E., Ahn, Y.J., Park, S.: A study on the development of a training course for ship cyber security officers. J. Korean Soc. Mar. Environ. Safety **26.7**, 830–837 (2020). https://doi.org/10.7837/kosomes.2020.26.7.830
76. Lee, Y.C., et al.: Improving cyber security awareness in maritime transport?: a way forward. J. Korean Soc. Mar. Eng. **41.8**, 738–745 (2017). https://doi.org/10.5916/jkosme.2017.41.8.738
77. Liberia, M.A.: Marine Notice RLM-118 Requirements for merchant marine personnel certification. Monrovia, Liberya, 2021. https://www.liscr.com/download/file/fid/5168 (visited on 09/20/2022)
78. Limoncelli, T., Hogan, C., Chalup, S.: Practice of System and Network Administration. 3rd ed. Addison-Wesley Professional, 2016
79. Lovell, K.N., Heering, D.: Exercise Neptune: Maritime cybersecurity training using the navigational simulators. In: 5th Interdisciplinary Cyber Research Conference. 2019
80. LR. Maritime cyber security awareness. https://www.lr.org/en/training/understandingrules-and-regulations/maritime-cyber-security-awareness/ (visited on 09/28/2022)
81. Lumivero. Citavi - The only all-in-one writing and referencing solution. 2023. https://lumivero.com/products/citavi/ (visited on 09/26/2023)
82. Marshall Islands Maritime Administrator. MI-118 Requirements for seafarer certification. 2021. https://www.register-iri.com/wp-content/uploads/MI-118.pdf (visited on 09/20/2022)
83. Meland, P.H., et al.: A retrospective analysis of maritime cyber security incidents. TransNav Int. J. Mar. Navig. Saf. Sea Transp., 153, 519–530. (2021). https://doi.org/10.12716/1001.15.03.04.
84. Mindykowski, J. (2014) MET standards for electro-technical officers. TransNav Int. J. Mar. Navig. Saf. Sea Transp., 84, 587–590. (2014). https://doi.org/10.12716/1001.08.04.14
85. Mirriahi, N., Alonzo, D., Fox, B.: A blended learning framework for curriculum design and professional development. Res. Learn. Technol. (2015). https://doi.org/10.3402/rlt.v23.28451
86. Mission Secure. A comprehensive guide to maritime cybersecurity. 2020. https://www.missionsecure.com/hubfs/Assets/eBooks/A%20Comprehensive%20Guide%20to%20Maritime%20Cybersecurity_Final.pdf (visited on 10/26/2022)

87. MITAGS. Cyber skilled mariner call to action day. 2022. https://www.mitags.org/course/cyberskilled-mariner-call-to-a-action-day/ (visited on 09/28/2022)
88. MITAGS. Maritime cyber security. 2022. https://www.mitags.org/course/maritime-cybersecurity/ (visited on 09/28/2022)
89. MITRE ATT&CK^{R}. https://attack.mitre.org/. Accessed on 02 Sep 2023
90. MPA. Notations for Singapore Registry of Ships (SRS Notations). 2022. https://www.mpa.gov.sg/singapore-registry-of-ships/about-srs/srs-notation (visited on 10/30/2022)
91. MPA. The application form and checklist for SRS notations. 2022. https://go.gov.sg/srsnotationapplication (visited on 10/30/2022)
92. MTS. Cyber security CBT. https://www.maritimetraining.com/Course/Cyber-Security-CBT (visited on 12/11/2022)
93. Nadler, L.: Designing training programs: The Critical Events Model. Addison-Wesley Publishing, US (1982)
94. Nautical Institute. Maritime cyber awareness for seafarers. 2022. https://www.nautinst.org/niacademy/other-provider-courses/maritime-cyber-awareness-for-seafarers.html (visited on 09/28/2022)
95. Nautical Institute. Maritime cyber awareness for seafarers. 2022. https://www.nautinst.org/shop/maritime-cyber-awareness-for-seafarers.html (visited on 09/28/2022)
96. NTNU. TS501822 - Maritime Digital Security. https://www.ntnu.edu/studies/courses/TS501822/2022/ (visited on 02/04/2023)
97. Rob O'dwyer. NYK Line oil tanker gets first ClassNK cyber notation. 2021. https://smartmaritimenetwork.com/2021/11/10/nyk-line-oil-tanker-gets-first-classnk-cybernotation/ (visited on 07/30/2022)
98. O'Neill, G.: Curriculum design in higher education: Theory to practice. 1st ed. Dublin, Ireland: University College Dublin, 2015. ISBN: 9781905254989. https://researchrepository.ucd.ie/handle/10197/7137 (visited on 11/01/2022)
99. Ocean Technologies Group. Cyber Security at Sea. 2022. https://library.oceantg.com/learningtitle/9d5e6fbd-f48e-4293-a288-172de63cd61f (visited on 09/28/2022)
100. OCIMF. Ship Inspection Report (SIRE) Programme. London, UK, 2018. https://www.ocimf.org/document-libary/287-sire-vessel-inspection-questionnaire-viq-ver-7007-questionnaire/file (visited on 10/25/2022)
101. OCIMF. SIRE 2.0 question library: Part 1 - Chapters 1 to 7. London, UK, 2022. https://www.ocimf.org/document-libary/630-sire-2-0-question-library-part-1-chapters-1-to-7-version-1-0-january-2022/file (visited on 11/11/2022)
102. OCIMF. The Tanker Management and Self-Assessment (TMSA) 3. A best practice guide. Scotland, UK, 2017
103. Allan, C., Ornstein, H., Francis, P.: Curriculum: Foundations, principles, and issues. 7th ed. Harlow, England: Pearson Education, 2017. ISBN: 978-1-292-16207-2
104. Oruc, A.: Claims of state-sponsored cyberattack in the maritime industry. In: The International Naval Engineering Conference and Exhibition (INEC 2020). 2020
105. Oruc, A.: Ethical considerations in maritime cybersecurity research. TransNav Int. J. Mar. Navig. Saf. Sea Transp., **16.2**, 309–318. (2022). https://doi.org/10.12716/1001.16.02.14.
106. Oruc, A.: Tanker industry is more ready against cyber threats. In: International Conference on Marine Engineering and Technology Oman 2019 (ICMET Oman). 2019. https://doi.org/10.24868/icmet.oman.2019.030.
107. Oruc, A.: Tools for organizing an effective virtual academic conference. Ser. Rev. **47.3–4**, 231–242 (2021). https://doi.org/10.1080/00987913.2022.2050615
108. Oxford. Knowledge noun. https://www.oxfordlearnersdictionaries.com/definition/english/knowledge?q=knowledge (visited on 11/05/2022)
109. Oxford. Skill noun. 2022. https://www.oxfordlearnersdictionaries.com/definition/english/skill?q=skill (visited on 11/05/2022)
110. Parson, L., Weise, J.: Postcolonial Approach to Curriculum Design. In: Parson, L., Casey Ozaki, C. (eds.) Teaching and learning for social justice and equity in higher education, pp. 93–116. Springer International Publishing, Cham (2020)
111. Potamos, G., Peratikou, A., Stavrou, S.: Towards a Maritime Cyber Range training environment. In: 2021 IEEE International Conference on Cyber Security and Resilience (CSR). 2021, pp. 180–185. https://doi.org/10.1109/CSR51186.2021.9527904.
112. Prasanna, S.D.: The different ranks of seafarers. 2011. https://toughnickel.com/industries/ranksofseafarersresponsibilities (visited on 09/20/2022)
113. Prideaux, D.: ABC of learning and teaching in medicine. Curric. Des. BMJ **326**(7383), 268–270 (2003). https://doi.org/10.1136/bmj.326.7383.268
114. Republic of the Marshall Islands Maritime Administrator. Maritime cyber risk management resources. 2021. https://www.register-iri.com/wp-content/uploads/SS-200-Maritime-Cyber-Risk-Management-Resources.pdf (visited on 11/06/2022)
115. RightShip. RightShip Inspection Ship Questionnaire (RISQ) 3.0. London, UK, 2023. https://explore.rightship.com/RISQ (visited on 07/23/2023)
116. RINA. Cybersecurity in maritime industry. https://www.rina.org/en/maritime-cyber-riskmanagement (visited on 09/26/2022)
117. Safety4Sea. BV awards cyber security notation to LNG carrier. 2020. https://safety4sea.com/bvawards-cyber-security-notation-to-lng-gas-carrier/ (visited on 07/30/2022)
118. Safety4Sea. Lloyd's Register gives world's first Cyber SAFE notation. 2017. https://safety4sea.com/lloyds-register-gives-worlds-first-cyber-safe-notation/ (visited on 07/30/2022)
119. Schagaev, I., Bacon, E., Ioannides, N.: An approach to curriculum design for computer science. In: Knowledge Management, Information Systems, E-Learning, and Sustainability Research. Ed. by Miltiadis D. Lytras et al. Vol. 111. Communications in Computer and Information Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 493–499. ISBN: 978-3-642-16317-3. https://doi.org/10.1007/978-3- 642-16318-0_63
120. Shapo, V., Levinskyi, M.: Means of Cyber Security Aspects Studying in Maritime Specialists Education. In: Auer, M.E., Tsiatsos, T. (eds.) Internet of Things, Infrastructures and Mobile Applications, pp. 389–400. Springer International Publishing, Cham (2021)
121. Shipping.fo. Accounting. 2020. https://www.shipping.fo/accounting (visited on 09/19/2022)
122. Singh, G.D.: The ultimate Kali Linux Book: Perform advanced penetration testing using Nmap, Metasploit, Aircrack-ng, and Empire. 2nd ed. Packt Publishing, 2022
123. Singh, S., et al.: Improving outcomes and reducing costs by modular training in infection control in a resource-limited setting. Int. J. Qual. Health Care **246**, 64.1-648 (2012). https://doi.org/10.1093/intqhc/mzs059
124. Skulmoski, G.J., Hartman, F.T., Krahn, J.: The Delphi method for graduate research. J. Inf. Technol. Edu. Res. **6.1**, 1–21 (2007)
125. Solent University. Cyber security for maritime professionals. https://maritime.solent.ac.uk/courses/stcw-safety-and-security/cyber-security-maritime-professionals (visited on 09/26/2022)
126. Solent University. Deck officers. https://maritime.solent.ac.uk/careers/career-progression-and-advice/deck-officers (visited on 09/15/2022)
127. Solent University. Engineer and electro-technical officers. https://maritime.solent.ac.uk/careers/career-progression-and-advice/engineering-eto-officers (visited on 09/15/2022)

128. Solent University. Proficiency in cyber security hygiene. https://maritime.solent.ac.uk/courses/stcw-safety-and-security/proficiency-in-cyber-security-hygiene (visited on 09/26/2022)
129. Solent University. Ship cyber security officer. https://maritime.solent.ac.uk/courses/stcwsafety-and-security/ship-cyber-security-officer (visited on 09/26/2022)
130. Sparhawk and Sally: Identifying targeted training needs. Jossey-Bass, San Francisco, California, USA (1994)
131. TalTech. Introduction to Cyber Security. https://ois2.ttu.ee/uusois/subject/VLL1480 (visited on 02/04/2023)
132. TalTech. Maritime cybersecurity. https://taltech.ee/en/estonian-maritime-academy/areasof-advance/maritime-cyber-security (visited on 09/26/2022)
133. Maritime Trainer. Cyber security. 2022. https://www.maritimetrainer.com/product/cybersecurity/ (visited on 09/28/2022)
134. UNCTAD. Review of maritime transport 2021. New York, USA, 2021. https://unctad.org/webflyer/review-maritime-transport-2021 (visited on 11/20/2021)
135. University of Plymouth. Cyber security awareness course for seafarers. https://www.plymouth.ac.uk/whats-on/cyber-security-awareness-for-seafarers (visited on 09/26/2022)
136. UNSW. Case studies. 2020. https://www.teaching.unsw.edu.au/case-studies (visited on 11/06/2022)
137. USCG. CVC-WI-27(2) Vessel cyber risk management work instruction. Washington, USA, 2022. https://www.dco.uscg.mil/Portals/9/CVC-WI-27%282%29.pdf (visited on 11/06/2022)
138. Williams, R.: Gard guidance on maritime claims and insurance. 2013. https://www.gard.no/Content/20823111/Gard%20Guidance%20on%20Maritime%20Claims_final.pdf (visited on 09/23/2022)
139. Witherbys, BIMCO, and ICS. Cyber security workbook for on board ship use. 2022
140. YouTube. Cyber security summer school 2018. 2019. https://www.youtube.com/watch?v=zKyUBGgDvUI (visited on 09/26/2022)