TRANSNAV
http://ww.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 18
Number 4
December 2024
DOI: 10.12716/1001.18.04.01

Evaluation of Maritime Cyber Security (MarCy) Training Programme

A. Oruc, N. Chowdhury, V. Gkioulos & S. Katsikas
Norwegian University of Science and Technology, Gjøvik, Norway

ABSTRACT: The prevalence of digital technologies is growing in the maritime industry, as in other sectors. Consequently, concerns regarding cyber risks are also escalating. Incidents have occurred in the industry, and findings from academic studies further validate these concerns. While technical measures are being taken against cyber threats, the human element remains another crucial aspect that requires strengthening. To effectively combat cyber threats and vulnerabilities, it is imperative to enhance individuals' awareness through education and training. In order to address the cyber security training needs of maritime professionals and students, we have developed an approach called the Maritime Cyber Security (MarCy) training programme. In this study, we evaluate all stages of the proposed programme through four conducted training sessions involving different learner groups. As a result, the MarCy programme was improved based on the findings obtained during the training sessions and the feedback from the learners. This study validates that the MarCy programme is an effective approach to meet the cyber security training needs of various groups in the maritime domain.

1 INTRODUCTION

Sea transport handles over 80% of the global merchandise trade volume [42], and as a result, the maritime industry has become a vital sector with millions of professionals working in it. The number of seafarers alone is approximately 1.9 million [2]. The Standards of Training Certification and Watchkeeping (STCW) Code currently lacks any requirements or recommendations for enhancing the cyber awareness of seafarers. Therefore, seafarers, beyond the training requirements of the International Maritime Organization (IMO), typically receive cyber security training during their professional careers. However, the possibility of this situation changing is likely. The Republic of Korea submitted a proposal in December 2021 to discuss the importance of integrating cyber security training into the STCW [18]. The Sub-committee on Human Element Training and Watchkeeping at the IMO was invited to deliberate on relevant provisions concerning training for seafarers in the field of cyber security.

We developed the MarCy training programme by incorporating the insights and opinions of experts, with the aim of its application in maritime cyber security training courses. The purpose of this study is to evaluate the applicability and effectiveness of the MarCy training programme. This work is a continuation of our previous work proposed by Oruc, Chowdhury, and Gkioulos [30]. The contribution of our study can be summarized as follows.

– evaluation of the MarCy training programme: The essential contribution of the paper is the development, evaluation, and validation of the MarCy training programme. The authors

organized and executed four distinct training sessions involving various learner groups. Through these training sessions, the authors effectively evaluated and refined all phases of the MarCy training programme based on empirical findings and feedback from the participants.
- evaluation of training sessions: In the original study [30], there were limited recommendations for evaluating a training program. However, in this study, the conducted training sessions were comprehensively assessed from various aspects. The evaluation approach presented in this publication can also be employed to assess training programs designed using methods other than the MarCy programme.
- sharing observations and participants' feedback: Through the organized training sessions, insights were gathered from academics, students, and industry professionals regarding maritime cyber security. Alongside the authors' observations, participants' perspectives are shared in the paper. Thus, this study contributes to bridging the gap between academia and industry.

In summary, our study presents the MarCy training programme, developed with expert insights for application in maritime cyber security training. Through the evaluation of training sessions, we enhance the programme's effectiveness. This work builds upon our prior research [30]. Our contributions encompass a comprehensive assessment of the programme and training sessions, enabling adaptable evaluation methodologies. Sharing participants' feedback and observations further facilitates academia-industry collaboration. Overall, our study enriches maritime cyber security training by providing a refined programme and a holistic approach to training evaluation.

In this study, the MarCy programme was implemented to develop cyber security training courses for students and professionals. Before the training courses, a pre-requisite survey was conducted by holding a meeting with the leaders of partner organizations. Subsequently, partners sent another pre-requisite survey to invitees to gather their training expectations. The training planning was conducted, considering the expectations of invitees and leaders, and the training was provided accordingly. During training sessions performed, a post-assessment survey was performed for learners to evaluate the effectiveness of the training.

In this study, the term partner refers to an organization (e.g., a class society) with whom we conducted training sessions collaboratively. A leader represents an individual (e.g., a manager) who was responsible for organizing the training courses on behalf of the partner organization. A learner denotes a participant (e.g., a student) who attended the conducted training course. An invitee refers to an individual who has responded to the pre-requisite survey.

While the MarCy programme has the potential for expansion with additional modules to cater to various stakeholders in the maritime industry, the focus of the original paper is specifically on the implementation of cyber security training for seafarers and office staff in shipping companies. This study demonstrates the application of the MarCy programme in the training of students from different departments (both maritime and non-maritime), office employees in shipping companies, and technical staff from class societies. Even though this study does not cover the training of all professional groups, such as port employees, navy personnel, and civil servant in maritime administrations, it is possible to implement the MarCy programme to provide cyber security training for these groups, addressing the specific cyber risks in the maritime domain. The values indicated by percentages in the study may be rounded without altering the findings. For instance, the value of 43.8% may be expressed as 44%.

The rest of this paper is structured as follows. Section 2 summarizes the MarCy training programme. In Section 3, related works in the literature are examined. The methodology employed in this study is outlined in Section 4. Section 5 presents the observations and findings. Lastly, in Section 6, a summary is provided, along with recommendations for additional research questions to be explored in the future.

2 BACKGROUND

Over the years, several models have been put forth to guide the design and development training programs. One such model is the Critical Events Model (CEM) introduced by Leonard Nadler in 1982, which has acquired recognition as a well-established and extensively described approach to training design. The CEM provides a comprehensive framework for designing training courses. It is not limited to formal education settings, but can also address the training requirements of various organizations. Notably, the CEM is well-suited for industries characterized by rapid changes, offering a flexible and adaptable approach. [25]

CEM is an effective model for designing training. We have made three modifications to CEM with the MarCy programme. Firstly, CEM does not have a modular approach. However, the modular approach of the MarCy programme allows customization of training by individual needs. While CEM can be used to design training for various industries, the designers must have a good understanding of the industry's needs and how to meet them. The MarCy programme is specifically designed to address the cyber security needs of maritime professionals and students. Therefore, even if training designers do not have an in-depth knowledge of maritime cyber security, they can still design effective training by following the phases outlined in the programme. It serves as an effective guide for a training designer. Lastly, while CEM relies on obtaining expert opinions at each phase of training design, the MarCy programme has already been evaluated by experts using the Delphi method. Furthermore, the programme is built upon the improvement of designed training through observations and implementing quantitative and qualitative assessments.

The modular training approach involves offering learners relevant components of a training program tailored to their individual training needs. This

approach has been implemented for various training requirements and has proven particularly effective in vocational training [16, 11]. By providing attendees with only the necessary knowledge aligned with their learning needs, this approach minimizes disruptions to their professional lives. Consequently, modular training is a cost-effective method that can be delivered online, offering flexibility to both the training designer and the learner [39]. This approach allows the designer to incorporate new modules, enabling the provision of updated qualifications for instructors. As a result, the training can easily adapt to the evolving needs of the industry, ensuring a responsive approach to changing training requirements [16].

By integrating a modular training approach into the CEM, we have made modifications to cater to the specific needs of the maritime industry. Through our modifications, professionals in the maritime domain can have the flexibility to select and complete only the modules that are relevant to their specific roles and responsibilities. Furthermore, the application scope of the programme has been expanded. By developing additional modules, we have extended the training opportunities to encompass various professionals within the maritime domain, including seafarers, office staff, port employees, navy personnel, and so on. This allows for the delivery of specialized cyber security training that meets the specific requirements of each professional group.

The CEM incorporates evaluation as a crucial component in assessing outcomes and objectives during the training design process [25]. The model includes a self-evaluation phase, where discussions with internal and external experts take place after each step. In practice, this requires a minimum of eight meetings with experts to evaluate a training program being developed. However, maritime cyber security is relatively a new domain. Bolbot et al. [4] highlights that there has been an increase in academic publications on maritime cyber security since 2017, while Oruc [29] indicates that public interest in maritime cyber security has started to grow in the same year and provides an explanation for this trend. Taking into account the emphasis on the year 2017 in both studies, it can be inferred that the global pool of maritime cyber security experts is still limited. Additionally, arranging meetings with selected experts poses challenges in terms of scheduling and time constraints for training development.

To address these limitations, we have replaced the original evaluation phase of the CEM with our evaluation approach. Our proposed approach still relies on feedback from relevant stakeholders but focuses exclusively on internal stakehold- ers involved in the training process. This approach simplifies data collection while ensuring that the developed training is customized and targeted to the needs of the participants. As a result of our modifications, we present a programme for maritime cyber security training, as depicted in Table 1.

We employed the Delphi method to evaluate the MarCy training programme. The Delphi method is widely recognized in the literature as a suitable research instrument for gathering judgments and opinions on topics where knowledge may be incomplete [40]. This method involves an iterative process that aims to collect feedback from a selected panel of experts who provide their insights anonymously. The Delphi method has evolved over time, allowing for increased flexibility in its implementation.

Table 1. Phases of the MarCy Training Programme [30]

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 learners 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 analyzed.
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.

We chose the Delphi method as the validation technique for our programme because it enables us to gather weighted feedback from the panel of experts and facilitates open debate without the need for practical evaluation methods such as experimentation. This approach proved beneficial in collecting valuable insights and opinions from a diverse group of experts, contributing to the refinement and validation of our training programme.

Table 2. Training Modules with their Objectives [30]

Code	Title	Objective
M1	Basic cyber security	The attendees will be familiar with the basics of cyber security.
M2	Advanced cyber security	The attendees will have advanced knowledge of cyber security.
M3	Regulatory requirements	The attendees will learn regulations for cyber security.
M4	Vetting requirements	The attendees will learn cyber security requirements in vetting programmes.
M5	Critical deck systems	The attendees will learn cyber risks in the critical deck systems.
M6	Critical engine systems	The attendees will learn cyber risks in the critical engine systems.
M7	Other critical systems	The attendees will learn cyber risks in other critical systems.
M8	Cyber security investments	The attendees will be able to decide cyber security investments.
M9	Cyber security practices	The attendees will have practical experience in implementation.
M10	Cyber security management	The attendees will be able to manage cyber security issues in a company.
M11	Advanced skills	The attendees will have advanced technical skills.

3 RELATED WORK

Erstad et al. [14] explore the application of a Human-Centered Design (HCD) approach for maritime cyber resilience training. The authors propose using HCD for the development of tailored maritime cyber resilience training, including simulator-based team training. By engaging with end-users and incorporating learning theories, the training becomes

realistic and relevant to the learners' needs. The paper justifies the use of HCD based on constructivism and connectivism learning approaches, which are commonly employed in maritime simulator training. The authors argue that the HCD process is effective despite its time-consuming nature.

Canepa et al. [7] examine the challenges of maritime cyber security training and the use of a cyber range as a solution. It provides a literature review on cyber security education and training, with a specific focus on the maritime domain. The paper presents the Cyber-MAR project [10], which implements a federated cyber range solution as part of a cyber security training platform tailored to the maritime sector. The methodology includes qualitative analysis through literature review and analysis of target groups, as well as quantitative analysis of the results from the initial Learning Management System (LMS) training. The findings highlight that most participants experienced improved cyber security skills and increased awareness of cyber threats.

Potamos et al. [37] present a novel training curriculum and offer design guidelines for creating activities on a maritime cyber range, with the aim of strengthening defenses against ransomware attacks. An important aspect of the curriculum is its emphasis on structured walkthrough practice, which encourages active learning and enhances the practicality and memorability of the educational experience. The proposed curriculum seeks to provide design guidance to the cyber security community for developing future training programs that specifically address the challenges posed by ransomware attacks.

La Vallée et al. [21] discuss maritime-specific training conducted through a federation of cyber ranges. The training scenario involves interconnected cyber ranges designed to support a complex defensive exercise. The technical challenges of federating cyber ranges, such as preserving network address ranges and configuring routing, were successfully addressed. The training covers various aspects of defensive actions, focusing on the impact of the Electronic Chart Display and Information System (ECDIS) console infection on the navigation system, analysis of traffic traces facilitated by the Security Operation Centre (SOC) server, and the repercussions of mis-configured firewalls and delayed vulnerability patching. The training emphasizes the importance of good security practices to enhance the overall security posture of systems, particularly in the maritime domain.

The research project Addressing Cyber Security in Maritime Education and Training (CYMET) by the International Association of Maritime Universities (IAMU) aims to enhance cyber awareness in the maritime industry through education and training [1]. The project evaluated the training needs of seafarers and provided recommendations for maritime education and training. A web-based training solution was proposed using Moodle [24] and itsLearning [38] platforms. The training package includes seven lessons covering various aspects of cyber security, such as cyber threats, organizational awareness, security management, good practices, rules, standards, and real-life examples. Additional lessons on network integrity, Global Positioning System (GPS) jamming and spoofing attacks, and safe information exchange were also included. The web-based course was tested with a pilot group of cadets, and feedback indicated that the course was effective and engaging for the participants.

Chowdhury and Gkioulos [8] performed a study to develop and evaluate two participant-centered cyber security training exercises using the Personalized Learning Theory (PLT)-based training framework. The exercises involved 12 master's students from the Norwegian University of Science and Technology (NTNU) and included game-based scenarios using CybeCIEGE and a physical table-top team exercise. The table-top exercise was specifically developed to tackle gaps highlighted when reviewing participant's performance in CyberCIEGE, and followed a turn-based format, modeled after the Lockheed Martin cyberkill chain. Evaluation of both exercises showed that participants' engagement and motivation increased as they were involved in exercise development, leading them to use the training tools independently. CyberCIEGE was particularly effective for learning cyber security concepts. Exercise duration affected participants' fatigue. Qualitative evaluation showed that the PLT-based model outperformed other, more traditional assessment methods.

In the exercises organized by Chowdhury and Gkioulos [8], pre & post-assessment surveys were conducted with the learners. Initially, a survey-based pre-requirement assessment was performed to the participants. Based on the collected feedback, exercise resources and test cases were developed. The post-assessment survey gathered feedback from the learners regarding all stages of the training. Furthermore, at the conclusion of the conducted training, it was discussed with the participants. Throughout the training, the instructor observed all participants and recorded findings. In our own training sessions, we have developed a similar approach tailored to our needs. The key difference is the implementation of exams administered before and after the training, enabling us to better evaluate the effectiveness of the training.

The literature review revealed that there is a scarcity of both theoretical and practical scientific publications on maritime cyber security training. Furthermore, to the best of our knowledge, there is no existing literature specifically addressing cyber security training needs for technical staff of class societies. Typically, applied research studies focus on students or seafarers. With this study, our aim is to address the aforementioned gaps in the literature. Lecturers can create or improve their training lectures based on the findings and observations we have obtained.

4 METHODOLOGY

In this study, the MarCy programme is implemented and evaluated, with a particular focus on evaluating leaders', learners', and invitees' engagement and feedback. To this end, the following process was pursued to make quantitative and qualitative

analyses. A graphical representation of the methodology followed is shown in Figure 1.

- identification of partners;
- performing pre-requisite surveys for leaders and invitees;
- analysis of training expectations;
- development of materials such as presentations and post-assessment surveys;
- performing training and post-assessment surveys;
- analysis of exams, evaluations, and feedback;
- improvement of the MarCy training programme.

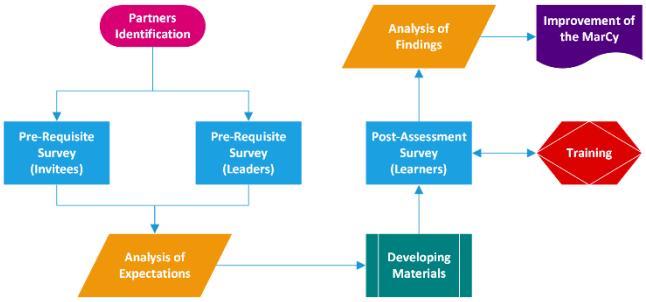

Figure 1. Methodology

For the purpose of evaluating the effectiveness of the MarCy training programme, we decided to conduct training sessions. To facilitate this process, we actively sought out partners who would collaborate with us in organizing the training. In selecting our partners, we placed importance on ensuring a diverse range of potential learner profiles. Specifically, we aimed to avoid partnering with organizations that shared similar learner groups. By adopting this approach, we were able to gather feedback from various learner groups. Ultimately, we successfully established partnerships with four organizations: a class society, a student club affiliated with a university, a maritime faculty, and a maritime training company.

After determining our partners, we prepared two different pre-requisite surveys to understand the training needs and expectations. One of these surveys was designed for the leaders of our partners, while the other was aimed at invitees. By conducting these two surveys, our aim was to understand whether there were any differences in perspectives between the leaders and the invitees.

Firstly, we conducted separate meetings with the leaders of our partners to perform pre-requisite surveys, each lasting 2.5 hours. The leaders who participated in these meetings are shown in Table 3. Some leaders partially attended the meetings due to their work schedules. Except for the Maritime Faculty, the meetings were conducted with the participation of 2-5 leaders. For the Maritime Faculty, the training was delivered within a formal lecture, Safety at Sea. Thus, the pre-requisite survey was held solely with the course lecturer. During these meetings, we asked the questions from the pre-requisite survey prepared for the leaders of the partners [32]. These questions were divided into five categories: identification of the background of the organization, thoughts on an ideal maritime cyber security training, preferences of the partner for the upcoming training (e.g., modality, language, and training duration), identification of the needs of the organization, roles and responsibilities of potential learners, and feedback about the curriculum of modules.

The pre-requisite survey for invitees was prepared as an online survey (and its access link was shared through leaders with invitees (PDF version of the survey: [31])). The survey comprised two sections: identification of the background and identification of training expectations. Despite reminders, an insufficient number of invitees filled out the pre-requisite survey. The number of invitees who filled out the pre-requisite survey is provided in Table 3.

Table 3. Leader Profiles and Invitees Numbers attended Pre-Requisite Survey

Partners	Pre-Requisite Survey Leaders	Invitees
class society	managers & technical staff	3
maritime faculty	course lecturer	0
student club	club leaders (students)	19
training company	top management & managers	16

During the identification of training needs, analyses were conducted by considering the pre-requisite surveys filled out by invitees invited by the Student Club and Training Company, as well as through meetings with leaders. Because of a significantly low response number to the survey, the responses of Class Society's invitees were not considered.

After analyzing the training expectations of leaders and invitees, the training sessions were planned. Firstly, the presentations to be used in training sessions were prepared. Then, specified post-assessment surveys were developed based on potential learner profiles and the training modules to be provided (e.g., the post-assessment survey specified for the Class Society [33]). The post-assessment survey consisted of five sections: learner identification, Quiz, feedback on the modules, Test, and feedback on the training. In this study, the Quiz refers to the exam conducted before the training, while the Test represents the exam performed after the training.

Through the post-assessment survey, information about the learners' background was collected and the questions in the Quiz were answered by learners prior to the training. Then, the training modules were delivered by the instructors. After each module, learners were asked to evaluate the module. After all modules were covered, learners answered the questions in the Test. Finally, the overall training was evaluated by the learners. The conducted training sessions were analyzed, considering the observations of the instructors, evaluations, feedback, and exam results in the post-assessment survey. Finally, the MarCy programme was improved based on the findings and feedback obtained.

Nettskjema [43], a web-based survey tool developed and designed by the University of Oslo, was used to collect responses from online participants (invitees & learners) for pre-requisite and post-assessment surveys. For in-person learners, their responses were collected on paper and later transferred to Nettskjema by the instructor. In this way, the responses of all learners, both online and on-site, were merged on Nettskjema separately for each training session. Subsequently, the data obtained on

Nettskjema was exported in .xlsx file format (i.e., MS Excel), and the data were analyzed according to the objectives of the research. Definitions and descriptions collected from academic publications to support our study were extracted and managed using the Citavi software [9].

5 EVALUATION OF THE PROGRAMME

As stated in Section 4, initially, pre-requisite surveys were conducted with the leaders of all partners. It was observed during these meetings that the leaders lacked sufficient knowledge in the field of maritime cyber security. Therefore, it was necessary to provide them with detailed explanations regarding the questions included in the pre-requisite survey.

During the meetings conducted for the pre-requisite survey, we asked leaders questions to understand their thoughts on the knowledge level of potential learners regarding maritime cyber security. Global Navigation Satellite System (GNSS) attacks are one of the most common attacks in the maritime sector. Between February 2016 and November 2018 alone, 1311 vessels were affected by GNSS attacks [5]. All ship operators who hold a Document of Compliance (DOC) are required to comply with IMO's cyber security regulations [19]. Therefore, we asked our questions to the leaders regarding these two topics. We also included similar questions in the pre-requisite survey designed for the invitees. The questions we asked the leaders (A1, A2, A3) and the questions we asked the invitees (B1, B2, B3) are listed below, and their responses are shown in Table 4. As mentioned in Section 4, only the responses of the invitees from the Training Company and the Student Club were considered.

- A1. Do you believe that learners know what a GPS spoofing attack is?
- A2. Do you believe that learners are aware of the potential consequences of a GPS spoofing attack?
- A3. Do you believe that learners are aware of the cyber security requirements of IMO?
- B1. Are you aware of the GPS spoofing attack, which aims to provide incorrect location information to a GPS receiver?
- B2. Do you believe that you are aware of the potential consequences of a GPS spoofing attack?
- B3. Do you believe that you are aware of the cyber security regulations established by the IMO?

Some of the leaders of partners believed that some of the invitees were aware of GPS spoofing attacks, but none of the leaders believed that learners would be aware of the potential consequences. Except for the Student Club, our partners believed that invitees would generally be aware of IMO regulations. Some of the invitees expressed that they were aware of GPS spoofing attacks. When we asked those who were aware about the possible consequences of GPS spoofing attacks, we observed that approximately half (i.e., 25% of the total invitees) believed that they were aware.

We wanted to validate the thoughts of the leaders and invitees. Therefore, we looked at the answers to the questions in the Quiz conducted before the training. It is important to note that when comparing the profiles of the invitees and learners in Table 6, they are not identical. However, the results are significant in terms of providing insights.

The cyber security regulations of the IMO are described under the M3 Regulatory Requirements module, while the GPS spoofing attack is covered under the M5 Critical Deck Systems module. Both modules were provided to all partners' learners except for the Maritime Faculty, as they did not receive the M5 Critical Deck Systems module. Consequently, all learners, except those from the Maritime Faculty, had two questions regarding IMO cyber security regulations and one question about GPS spoofing attacks in their Quizzes. Learners from the Maritime Faculty were asked two questions related to IMO cyber security regulations in their Quiz. The percentages of correct answers for these questions are presented in Table 5.

Table 5. Correct Answer Percentage in Quizzes

	Class Society	Maritime Faculty	Student Club	Training Company
GPS spoofing attack	13%	N/A	50%	29%
IMO requirements	54%	43%	45%	73%

When analysing the provided responses, it can be observed that the thoughts of the invitees align approximately with the Quiz results of the learners. In other words, invitees are aware of what they know or don't know. Particularly, the results of the invitees from the Training Company were found to be very close (Pre-Requisite Survey: 68%, Quiz:73%). Since the invitees who participated in the pre-requisite survey and the learners who participated in the post-assessment survey are not exactly the same individuals, slight differences are expected. However, it appears that the leaders had more difficulty in predicting the knowledge levels of the potential learners. For instance, the leaders of the Student Club expected that none of the learners would be aware of IMO regulations, but the Quiz showed that approximately half of the learners were aware of these regulations.

During the pre-requisite survey conducted with the leaders, it was discovered that one of the partners had previously experienced a cyber attack. The Training Company provides maritime cyber security training to its customers online. The Class Society has provided a maritime cyber security training seminar to its technical staff in the past. The Student Club and Maritime Faculty have not provided maritime cyber security training before. On the other hand, we asked the similar questions in the pre-requisite survey prepared for the invitees. The responses of the invitees from the Training Company and the Student Club are included in Table 6.

- C1. Has your organization ever experienced any cyber attacks in the past?
- C2. Have you received any cyber security training specific to the maritime industry before?
- C3. If previously received, how much time do you allocate annually for maritime cyber security training?
- C4. Have you been a victim of any cyber attacks, such as malware (virus) infection, in your personal life?

Table 4. Leaders' and Learners's Opinions

Leaders' Opinion				Invitees' Opinion	
# Class Society	Student Club	Maritime Faculty	Training Company	# Student Club	Training Company
A1 Yes, some of them	Yes, some of them	No, none of them	No, none of them	B1 36% Yes, I am aware	32% Yes, I am aware
A2 No, none of them	No, none of them	No, none of them	No, none of them	B2 16% Yes, I am aware	25% Yes, I am aware
A3 Yes, most of them	No, none of them	Yes, some of them	Yes, all of them	B3 10% Yes, I am aware	68% Yes, I am aware

Table 6. Responses of Invitees

#	Student Club	Training Company
C1	0% Yes, it has been exposed. 42% No, it hasn't been exposed. 57% I don't know. / I prefer not to comment.	31% Yes, it has been exposed. 43% No, it hasn't been exposed. 25% I don't know. / I prefer not to comment.
C2	0% No one has received.	25% Yes, I have received.
C3	0% No one has received.	12% I allocate between 2 to 4 hours per year. 6% I allocate less than 2 hours per year. 6% I do not receive training annually.
C4	36% Yes, I have been exposed.	37% Yes, I have been exposed.

The invitees of the Student Club are university students. It is unlikely that a university has never experienced a cyber attack. However, the students may not be aware of potential attacks targeting their university, as it's possible that their universities have not recently faced major attacks that significantly impact the students. In contrast, the invitees of the Training Company are employees in maritime companies. Among them, 31% reported that their companies have been targeted by cyber attacks. While none of the Student Club's invitees have received any maritime cyber security training before, 25% of the Training Company's invitees have received such training in the past. Additionally, 12% of the Training Company's invitees receive maritime cyber security training for 2-4 hours annually. Both the invitees of the Student Club and the Training Company have personally experienced cyber attacks at a similar rate, with approximately 36% to 37% reporting such cyber incidents.

Table 7 presents the profiles of invited participants and learners according to their partners. As previously mentioned, when examining the profiles, differences were observed between those who responded to the pre-requisite survey and the post-assessment survey. The table shows the age, completed education level, professional background (for employees) and types of companies they work for, or departments (for students). The column "n" indicates the number of responses, while the "%" column represents the percentage of responses. The pre-requisite survey was completed by a total of 35 invitees from the Student Club and Training Company. All invitees of the Student Club (n=19) were undergraduate students studying in nine different departments, while all invitees of the Training Company (n=19) were professionals working in maritime companies. The post-assessment survey was answered by a total of 79 learners, with 54 being employees and 25 being students. The highest number of responses (n=31) came from the Training Company learners. It was observed that 74% of the Training Company learners had a deck background. Among the employees from Class Society, it was seen that 65% had a naval engineering background. It was observed that 74% of the Training Company learners were working in tanker operators and 35% working in dry cargo operators. (10% of the employees work for companies that operate both tanker and dry cargo ships.) All learners from the Maritime Faculty were studying in departments related to maritime studies, while learners from the Student Club were pursuing undergraduate education in different departments. The majority of employees had completed at least a bachelor's degree, while the majority of students had naturally not yet completed their high school education. In the following sections, considering the other findings, participants' responses (i.e., invitee & learner), and the observations of the instructor, all stages of the MarCy training programme will be evaluated. This will allow for addressing the identified shortcomings of the programme. Additionally, it will serve as a guide for course designers who wish to organize maritime cyber security training, enabling them to benefit from it.

5.1 *Identify the Needs of the Organization*

The goals of this step are to determine the nature of the problem [25]. For this stage, we first listened to the training needs for cyber security from leaders of our partners. We found that the stated needs were already covered by the content we recommended in the MarCy programme. Additionally, we observed that the leaders faced challenges in identifying their training needs because of their limited knowledge of maritime cyber security.

Next, we presented the existing training modules to leaders and gathered their feedback. Our partners' cyber security needs were easily identified with this method. We confirmed the modules specified in the MarCy programme met the needs of our partners, except for the Student Club. We noticed that the MarCy training programme did not fully address the training needs of the Student Club which was working on autonomous ship projects. As a result, we decided to develop the M12 Autonomous Ships module to cater to their specific needs.

The module selections of our partners' leaders are indicated with a "+" symbol in the "Leader" column of Table 8. As stated in Section 4, we were able to gather feedback from learners of two of our partners, Student Club and Training Company, for the pre-requisite survey. The module preferences of the invitees are expressed as percentages in the "Invitees" column.

Table 7. Invitee and Learner Profile by Partners

		Pre-Requisite Survey				Post-Assessment Survey							
		SC		TC		CS		SC		MF		TC	
Profile		n	%	n	%	n	%	n	%	n	%	n	%
AGE	between the ages of 18 and 25	18	94	1	6	1	4	10	100	15	100	3	10
	between the ages of 26 and 35	1	5	5	31	11	48					11	35
	between the ages of 36 and 50			10	62	9	39					16	52
	over 50 years old					2	9					1	3
EDUCATION	high school	15	78					10	100	13	87	2	6
	associated	1	5	4	25					1	7		
	bachelor	3	15	8	50	18	78			1	7	23	74
	master			4	25	4	17					5	16
	doctorate					1	4					1	3
BACKGROUND	deck			10	63	2	9					23	74
(if professional)	marine engineering					6	26						
	naval engineering					15	65					1	3
	computer science			1	6							3	10
	maritime business management			4	25							2	6
	human resources			1	6							2	6
COMPANY TYPE	tanker operator			7	44							20	65
	dry cargo operator			7	44							8	26
	tanker & dry cargo operator			1	6							3	10
	container & dry cargo operator			1	6								
	class society					23	100						
DEPARTMENT	naval architecture and marine eng.	2	10					1	10	4	27		
(if student)	marine engineering									11	73		
	shipbuilding and ocean engineering	5	26					2	20				
	mar. transpor. and management eng.							1	10				
	electrical engineering	3	15					2	20				
	electronics and communication eng.	1	5										
	control and automation engineering	3	15					1	10				
	mechanical engineering	2	10					1	10				
	mathematics engineering	1	5					1	10				
	artificial intelligence and data eng.	1	5					1	10				
	metallurgical and materials eng.	1	5										
Number of Invitees / Learners by Partners		19		16		23		10		15		31	
Total Number of Invitees / Learners		35 (16 emp. + 19 stu.)				79 (54 employees + 25 students)							

CS: Class Society | SC: Student Club | MF: Maritime Faculty | TC: Training Company
emp: employees | stu: students | eng: engineering | mar: maritime | transpor: transportation

While planning the training, we also tried to consider the training modules requested by more than 50% of the invitees who filled out the pre-requisite survey. Invitees from the Student Club, unlike the leaders, also requested the M3 Regulatory Requirements module. The invitees of the Training Company additionally requested the M2 Advanced Cyber Security module, but due to time constraints, we were unable to provide that module. Furthermore, the modules requested by the leaders and indicated with an "x" symbol in Table 8 were also not offered due to time limitations.

Further explanations regarding the training durations are provided in Section 5.8. The final decision for the training modules is shown in Table 8. Modules marked with "✓" and "⊕" symbols were delivered to the learners.

5.2 *Specify Job Performance*

The purpose of this step is to examine the roles and responsibilities of potential learners [25]. Having a clear understanding of the roles and responsibilities of learners is important for designing the training to cater to the specific needs of the overall learner group. The participation in the training organized by our partners was voluntary, meaning that we did not have precise knowledge of who would attend the training during the design phase, but we could make some predictions. The purpose of conducting the pre-requisite survey was to mitigate this uncertainty to some extent. However, participation in the pre-requisite survey was lower than expected. After the post-assessment survey, we gathered more information about the roles and responsibilities of the learners. As shown in Table 7, our partners' learners comprise both students and professionals. The roles of learners are presented in Table 9.

When designing the MarCy programme, we listed the possible responsibilities of professionals working in ship operators. The post-assessment survey, as indicated in the programme, revealed that the roles and responsibilities of individuals working in ship operators vary from company to company. We observed that employees might have combined roles such as "DPA & CSO". Therefore, the responsibilities of professionals might be also a combination based on roles.

Professionals working in ship operators participated in the training organized by the Training Company. Some of these learners were working in the crewing department. In our original study, we included the crewing department in "marine operations". However, the post-assessment survey showed that learners working in the crewing department had difficulty choosing marine operations for their responsibility. Instead, they added their responsibility such as "manning". On the other hand, we determined the roles and responsibilities of technical employees (e.g., surveyors) of class societies by considering the suggestion of the leaders of the Class Society. Possible roles and responsibilities for employees working in the crewing department of ship operators and technical staff of class societies are shown in Table 10.

Table 8. The Selection of Training Modules

	Pre-Requisite Survey									
	Leaders				Invitees		Final Decision			
Code Module	CS	MF	SC	TC	SC	TC	CS	MF	SC	TC
M1 Basic cyber security	+	+	+	+	78%	68%	✓	✓	✓	x
M2 Advanced cyber security	+	+	+		47%	68%	✓	✓	✓	
M3 Regulatory requirements	+	+		+	57%	62%	✓	✓	⊕	✓
M4 Vetting requirements	+	+		+	10%	68%	✓	✓		✓
M5 Critical deck systems	+		+	+	5%	87%	✓		✓	✓
M6 Critical engine systems	+	+		+	36%	43%	✓	✓		
M7 Other critical systems	+	+			42%	25%	x	x		
M8 Cyber security investments		+		+	21%	25%		x		✓
M9 Cyber security practices		+			31%	37%		x		
M10 Cyber security management	+	+		+	47%	50%	✓	x		x
M11 Advanced skills					47%	31%				
M12 Autonomous ships			+						✓	

+ Requested modules by leaders of partners.
✓ Requested modules by leaders of partners and given modules
x Requested by leaders of partners but wasn't given modules due to time limitation.
⊕ Requested by invitees (50%+) and given modules.

Table 9. Roles of Learners by Partners

Training Company	Class Society
operation manager	surveyor
operator	auditor
Designated Person Ashore (DPA)	plan approval engineer
DPA & CSO	quality engineer
training and marine superintendent	fleet monitoring manager
SHEQ manager	inspector
HSEQ & Cyber security manager	technical assistant
HSEQ superintendent	rule development engineer
HSEQ senior expert	
DPA & HSEQ manager	
deck superintendent	
deck superintendent & CSO	
safety superintendent	
marine superintendent	
DPA assistant	
crewing manager	
deputy crewing manager	
crew officer	
Information Technology (IT) staff	
training manager	

CSO: Company Security Officer
HSEQ: Health, Safety, Environment, and Quality
SHEQ: Safety, Health, Environment, and Quality

Table 10. Additional Roles and Responsibilities

Organization	Responsibility	Position (Role)
Class Society	survey & certification function	e.g., manager, surveyor, and auditor
Ship Operator	safe manning of ships	e.g., crewing department, crewing manager, crewing officer

5.3 *Identify Learner Needs*

The goal of this step is to comprehend the distinct learning requirements associated with each responsibility [25]. The MarCy programme provides training module recommendations based on the responsibilities of office employees working in ship operators. However, it is not mandatory to follow these recommendations. Module selections should be determined according to individuals' responsibilities.

We asked learners to answer the question "Did you find the training module relevant to your job responsibilities?" at the end of each module. The evaluations of company employees for each module are presented in Table 11. The responsibility of "safe manning of ships", as expressed in Section 5.2, has been added to this study after the training.

The responses of learners working in the crewing department have been taken into consideration for the responsibility of "safe manning of ships". Additionally, as mentioned in Section 5.2, employees can have multiple responsibilities. Table 11 was created considering only the responses of learners with a single responsibility. Considering the responses of learners with combined responsibilities would hinder establishing the relationship between responsibility and module. This is because the responses of learners with combined responsibilities may involve the influence of multiple responsibilities, which could make it more difficult to understand the relationship between responsibility and module. In contrast, the responses of learners with a single responsibility are more focused and can demonstrate the relationship more clearly.

Table 11. Module Evaluation based on Responsibilities of Office Employees

	M3		M4		M5		M8	
Responsibility	n	s	n	s	n	s	n	s
training activities	1	5.0	1	5.0	1	5.0	1	5.0
cyber security activities	0	-	0	-	0	-	0	-
IT activities	0	-	0	-	0	-	0	-
investments and management for marine operations	9	4.6	9	4.8	9	4.8	7	4.3
marine operations	10	4.7	9	4.4	9	4.7	9	4.4
support activities	0	-	0	-	0	-	0	-
safe manning of ships	3	5.0	3	4.7	3	3.7	2	3.5

n: number of responses | s: score | 5.0 is the highest score

Additionally, Table 12 presents the most useful and least useful modules as perceived by office employees based on their responsibilities. As mentioned earlier, in order to establish an accurate module-responsibility relationship, this table only considers the responses of learners with a single responsibility.

Table 12. The Most / Least Useful Modules by the Responsibilities of Office Employees

		Most Useful		Least Useful	
Responsibility	n	%	Module	%	Module
training activities	1	100	M4	100	M8
cyber security activities	0	-	-	-	-
IT activities	0	-	-	-	-
investments and management for marine operations	7	57	M4	71	M8
marine operations	9	44	M4	67	M8
support activities	0	-	-	-	-
safe manning of ships	3	67	M3	67	M8

n: number of responses

When considering the responses shown in Table 11 and Table 12, the need for M3 Regulatory Requirements and M4 Vetting Requirements training modules is required for the recently added responsibility of "safe manning of ships". Although our response count for the training activities responsibility is insufficient, there is no need for any changes in our original recommendations. Responses for "cyber security activities", "IT activities", and "support activities" responsibilities have not been considered as they are observed to be combined with other responsibilities assigned to employees. The M5 Critical Deck Systems module is not recommended in our original study for the "investment and management for marine operations" and "marine operations" responsibilities; however, learners have rated it 4.8 and 4.7 out of 5, respectively. This indicates that the MarCy programme needs to provide better recommendations.

Upon further examination, it is observed that all nine learners who indicated the "investment and management for marine operations" responsibility have a deck background. Out of the ten learners who mentioned the "marine operations" responsibility, eight have a deck background, while the remaining two have different backgrounds. Considering that most responses come from learners with a deck background, it is expected that there may be a need for training on different systems on the ship depending on the individual's background.

Considering the aforementioned points and the responses shown in Table 11 and Table 12, the module recommendations in the MarCy programme for office employees, based on their responsibilities, have been revised as seen in Table 13. In summary, the "investment and management" responsibility has been divided into two parts. It is stated that, depending on the employee's background, the M5 Critical Deck Systems, M6 Critical Engine Systems, or M7 Other Critical Systems training modules can be selected for the "management in marine operations" and "marine operations" responsibilities. The newly added responsibility of "safe manning of ships" has been included.

In the training conducted with Class Society, a total of 15 learners provided feedback on the most useful and least useful modules. Among the respondents, 40% identified the M3 Regulatory Requirements module as the most beneficial module, while 47% considered the M4 Vetting Requirements module as the least relevant to their roles. Additionally, 22-23 learners responded to the question, "Did you find the training relevant to your job responsibilities?" Based on the scores given to this question, the M4 Vetting Requirements module received the lowest score (3.6), as shown in Table 14. During the pre-requisite survey with the leaders of the Class Society, it was mentioned that the participants deemed the M4 Vetting Requirements module unnecessary and requested it solely for familiarization.

Table 13. Revised Training Module Suggestions by Responsibilities of Office Staff

Responsibility	Suggested Modules
training activities (e.g., training superintendent)	M1, M3, M4, M5, M6, M7
cyber security activities (e.g., Company Cyber Security Officer)	M1, M2, M3, M4, M5, M6, M7, M8, M9, M10, M11
IT activities (e.g., IT Operator)	M1, M2, M5, M6, M7
Investment (e.g., CEO and CFO)	M1, M3, M4, M8
management in marine operations (e.g., DPA and HSEQ Manager)	M1, M3, M4, M8 (elective by background: M5, M6, M7)
marine operations (e.g., HSEQ and marine superintendent)	M1, M3, M4 (elective by background: M5, M6, M7)
safe manning of ships (e.g., crewing manager)	M1, M3, M4
support activities (e.g., accounting manager)	M1
Additional responsibilities	Should be elected by considering individual responsibility. The potential modules include but are not limited to M1

Table 14. Module Evaluation based on responsibilities of Class Society Employees

	M1	M2	M3	M4	M5	M6	M10
n	23	23	23	23	23	23	22
score	4.1	4.0	4.3	3.6	4.0	4.2	4.1

n: number of responses | 5.0 is the highest score

According to the considerations mentioned above, the following training modules can be recommended for Class Society employees having the "survey & certification" responsibility: M1, M2, M3, M5, M6, M7, and M10 modules.

The training conducted with the Maritime Faculty and Student Club involved learners (i.e., students) from different departments, as shown in Table 7. Since they may take on various roles in the maritime industry after graduation, a specific evaluation of their responsibilities cannot be made. As seen in Table 15 and Table 16, the M3 Regulatory Requirements module was perceived as the least necessary training module by the learners from the Student Club. As shown in Table 7, it is worth noting that 60% of the Student Club participants are enrolled in non-maritime-related departments, which could explain why they found the M3 Regulatory Requirements module, which includes cyber security rules by IMO, to be the least useful. That's why we focused on only students studying in maritime departments (i.e., naval architecture and marine engineering, shipbuilding and ocean engineering, and maritime transportation and management engineering). According to the evaluations of the four learners who are studying in

maritime-related departments, the M1 Basic Cyber Security and M2 Advanced Cyber Security modules received 50% of the votes, indicating that they were perceived as the least useful modules. On the other hand, the students from the Maritime Faculty found all the training modules, including M3 Regulatory Requirements, to be useful.

Table 15. Students' Evaluation for Modules

	n	M1	M2	M3	M4	M5	M6	M12
Maritime Faculty	15	4.3	4.1	4.2	4.4	-	4.5	-
Student Club	10	4.2	4.4	3.3	-	4.5	-	4.7

n: number of responses | 5.0 is the highest score

The most useful and least useful modules according to learners of our partners are shown in Table 16. The M4 Vetting Requirements module was found to be the most useful by company representatives, while, as mentioned earlier, it was considered the least useful module by Class Society employees. A similar example can be observed with the M3 Regulatory Requirements module. While Class Society employees identified it as the most useful module, Student Club students expressed it as the least useful. Additionally, as seen in the Student Club training mentioned earlier, individuals with different educational backgrounds or training experiences may have varying training needs.

Table 16. Most / Least Useful Modules by Partners

	Class Society		Maritime Faculty		Student Club		Training Company	
	Module	%	Module	%	Module	%	Module	%
Most Useful Module	M3	40%	M6	40%	M12	50%	M4	44%
Least Useful Module	M4	47%	M1	33%	M3	40%	M8	63%

As suggested by credited maritime societies [3, 45, 28, 13], the MarCy programme advocates for cyber security training in the maritime domain to be tailored to individuals' roles and responsibilities rather than being generic. The evaluations provided by the learners after the training further confirm the validity of this recommendation.

5.4 *Determine Objectives*

The aim of this step is to establish the distinct goals and desired learning outcomes for each training module [25]. In our study, each module encompasses a unique objective. The learning outcome encompasses three key elements - knowledge, skill, and attitude - which collectively contribute to achieving the identified objectives. Knowledge is defined as "the state of knowing about a particular fact or situation" [34]. Skill is defined as "the ability to do something well" [35]. Attitude is defined as "a feeling or opinion about something, especially when this shows in your behaviour" [6]. The objectives and learning outcomes specified for the modules in the MarCy programme have been reviewed and confirmed by the leaders of our partners. As for the recently developed M12 Autonomous Ship module, the objectives and learning outcomes listed in Table 17 were determined based on the input of the leaders of the Student Club.

Table 17. Objectives and Learning Outcomes of the M12 Autonomous Ship Module

Code	Objective	K/S/A	Learning Outcome
M12	The potential cyber security risks of autonomous ships are understood.	K	- familiarity with autonomous ship projects; - published guidelines for autonomous ships; - cyber risk assessments for autonomous ships.

K: Knowledge | S: Skill | A: Attitude

5.5 *Build Curriculum*

The purpose of this phase is to construct a curriculum that aligns with the desired learning outcomes [25]. We consulted the leaders of partners regarding the curriculum and inquired about specific topics they wished to include. The MarCy programme not only offers modules but also provides curriculum recommendations, which largely meet the expectations of leaders of partners. However, we received some requests that included topics unrelated to cyber security, such as newly developed technologies in the maritime industry. We did not take these irrelevant expectations into consideration.

The M12 Autonomous Ship module was not included in the MarCy programme, so it was necessary to develop a curriculum for it. Considering the input of the leaders of the Student Club, we created a curriculum, as seen in Table 18. The contents are divided into two groups: essential and helpful. Essential content is crucial for achieving the objectives, while helpful content serves as an additional resource to complement the essential content [25]. Additionally, potential training materials that can be used for the module are listed in Table 18.

Due to time constraints, we needed to reduce the recommended curriculum of MarCy during training sessions. In our discussions with the leaders of partners, it was suggested to eliminate maritime-related notions and focus directly on maritime cyber security, considering that at least some learners already had foreknowledge. As a result, explanations of notions such as International Safety Management (ISM) Code, International Ship and Port Facility Security (ISPS) Code, and Ship Security Plan (SSP) were not covered, nor was there a general introduction to the systems on board the ship. Consequently, it was observed that learners, particularly those who had not received maritime-related education or were at the beginning of their maritime education, struggled to understand the topics. Therefore, when preparing a training curriculum, the MarCy recommends forming a learner profile consisting of individuals at the same level of knowledge. Another approach is to develop the training curriculum considering individuals with minimal familiarity with the subject, but this would inherently lead to an increase in the duration of the training.

The post-assessment survey revealed that learners expressed dissatisfaction due to certain topics not being covered in sufficient detail. It indicated that the recommended MarCy programme curriculum was not fully implemented, particularly in terms of the training duration being too short to adequately

address protection measures against cyber risks. The complaints raised by the learners served as the confirmation of the validity of the curriculum proposed by the MarCy programme.

Table 18. Curriculum and Potential Training Materials for M12 Autonomous Ship Module

Content	E/H	Material
autonomy classification of ships	H	[17]
autonomous ship projects	H	[15, 26, 27, 46]
standards and class guidelines	E	[12, 22]
attack surfaces	E	[41, 20, 36]
cyber risk assessment	E	[41, 20, 36]

E: essential content | H: helpful content

The MarCy training programme suggests prerequisite modules. Before enrolling in any other module, it is mandatory to complete M1 Basic Cyber Security. We continue to recommend this for the recently developed M12 Autonomous Ship module as well. However, we were unable to implement all of our prerequisite module recommendations in all training sessions. In the training conducted with the Training Company, the M1 Basic Cyber Security module was not delivered as the learners were already customers of Training Company, and they had received basic cyber security training from the company. Therefore, it was assumed unnecessary. In the training conducted with the Class Society, it was necessary to deliver the M7 Other Critical Systems and M9 Cyber Security Practices modules before the M10 Cyber Security Management module. Although the leaders of the Class Society requested the M7 Other Critical Systems module, it was removed from the training due to time management. The leaders also deemed the M9 Cyber Security Practices module unnecessary for their purposes.

5.6 *Select Instructional Strategies*

The goal of this phase is to ascertain the suitable teaching methods to be employed for the identified curriculum [25]. In the MarCy programme, five different instructional methods are suggested - lecture, case study, discussion, drill, and demonstration - could be used in maritime cyber security training.

We discussed the recommended instructional strategies of the MarCy programme with the leaders of partners. All of our partners agreed that the training can be delivered through lectures and case studies. They particularly emphasized that the case study method is highly effective in increasing participants' awareness.

The leader of Maritime Faculty expressed concerns that their students may be hesitant to participate in discussions because of embarrassment. The leaders of the Maritime Faculty and Student Club also stated that the demonstration method is not suitable for students as they do not have their own checklists, forms, or technical training facilities.

The leaders of the Class Society stated that their staff may not have sufficient knowledge of maritime cyber security, making it difficult for them to engage in discussions. The leaders of Class Society expressed that they did not require the drill method because they do not operate a vessel. However, it is important to note that cyber attacks can also target offices, and cyber security drills can be conducted in office environments as well. It is essential to ensure that all aspects of a maritime organization, including offices, should be prepared for and capable of responding to potential cyber threats.

Table 19 summarizes the ideal instructional methods for maritime cyber security training of invitees according to the perspectives of the leaders of the partners. In addition, the pre-requisite survey also asked the invitees about their preferred training methods. The preference rates of the invitees according to the strategies are shown in Table 19.

Both groups of invitees particularly supported the case study method for maritime cyber security training sessions. The invitees of the Training Company could not reach a consensus on other training methods. Most of the Student Club's invitees did not prefer the discussion and demonstration methods, which contradicts the views of the Student Club leaders. There was also no agreement among invitees of Student Club regarding the drill and lecture methods.

Lectures, case studies, and discussions of instructional strategies were implemented in our conducted training sessions. To apply the drill method, participants would have needed prior training aligned with the scenario, as they should have been aware of their roles and responsibilities during a cyber attack. However, our participant profile could not meet this requirement. For the demonstration strategy, it was necessary to have mutual forms and procedures among the participants, which were not available for our participant profile. Our inability to implement drill and demonstration methods in the conducted training session does not indicate that these methods are ineffective. Both methods can be effectively applied for the training of different learner groups, such as professionals working in the same shipping company or navy personnel.

We also gathered feedback from learners through a post-assessment survey regarding the instructional strategies. All learners found lecture, discussion, and case study methods to be effective. However, opinions regarding the drill and demonstration strategies varied. If we had the opportunity to implement the drill and demonstration methods as well, we expect that learners would have shown more interest in these methods. The learners' thoughts on instructional strategies are presented in Table 20.

Table 19. Ideal Instructional Strategies According to Leaders and Invitees

		Instructional Strategies				
Group	Partner	L	CS	Di	Dr	De
Leaders	class society	✓	✓			✓
	maritime faculty	✓	✓		✓	
	student club	✓	✓	✓	✓	✓
	training company	✓	✓	✓	✓	✓
Invitees	student club	52%	94%	21%	57%	31%
	training company	50%	93%	43%	43%	50%

L: Lecture; CS: Case Study; Di: Discussion; Dr: Drill; De: Demonstration

Table 20. Learners' Opinions on Instructional Strategies through Post-Assessment Survey

	Class Society		Maritime Faculty		Student Club		Training Company	
Instructional Strategy	E	I	E	I	E	I	E	I
Lecture	100%	-	100%	-	100%	-	100%	-
Discussion	100%	-	100%	-	100%	-	100%	-
Case Study	100%	-	100%	-	100%	-	100%	-
Drill	-	28%	-	73%	-	30%	-	37%
Demonstration	-	39%	-	73%	-	70%	-	52%

E: It was effective. | I: It should have been implemented.

In the post-assessment survey, we received many positive comments from the learners of all of our partners, particularly regarding the case study method. Unfortunately, obtaining detailed information about occurred cyber incidents in the maritime industry was challenging. The case studies explained during training sessions were found in documents [3] and [44].

5.7 *Obtain Instructional Resources*

The purpose of this stage is to verify that all the necessary resources for the training process are readily available [25]. This section emphasizes the importance of securing both physical and human resources, as well as ensuring the availability of training materials. The MarCy programme provides recommendations to instructors regarding potential disruptions that may occur during a training session. Particularly, issues related to physical resources were not a hindrance to the training sessions, as the provided recommendations were considered, regardless of the instructor.

5.7.1 *Training Materials*

PowerPoint presentations were prepared in English for training purposes. The content of the presentations consisted of books, academic publications, guidelines, circulars, videos, animations, and photographs. The prepared presentation was converted to PDF format with two slides per page and used as training material. A cover page was added to the material, which included an image related to training, training title, instructor identity, contact details, and training date. At the end of the material, a few pages of dot paper were added for participants to take notes.

The prepared training material was sent to partners approximately one week before the training. Depending on the number of modules, the training materials ranged from 70 to 100 pages. Because of the high page count, leaders of partners preferred to share the materials with invitees via e-mail or their own Learning Management System (LMS).

During the delivery of the training material, we observed some issues. Firstly, some learners expressed that they were unaware of the shared materials. Despite reminding one of our partners to send the training material one day before the training, they forgot to do so and could only send it during the training in response to requests from learners. It was discovered that some learners were unable to receive the material because of technical problems with e-mail delivery. The partner's e-mail address had been blacklisted by certain service providers, causing their e-mails to not reach any recipients. In some cases, the size of the material exceeded the limits allowed by the recipients' e-mail servers, resulting in direct rejection.

5.7.2 *Human Resources*

In the pre-requisite survey, the leaders of all partners expressed the need for the terminology to be provided in English during the training, but emphasized that the speech should be delivered in the native language of learners. They specifically highlighted the potential English proficiency issue of ratings, emphasizing the necessity of conducting the instruction in the native language.

Except for the Maritime Faculty, all of our partners' leaders requested that the instruction be conducted in the learners' native language. Therefore, the conducted training sessions were delivered in the learners' native language by a researcher specializing in maritime cyber security. Despite concerns from the leaders of the Maritime Faculty that the training might not be well understood by the learners (i.e., students), they requested that one module be delivered in English to enhance the students' understanding of the importance of English in the maritime industry. The M1 Basic Cyber Security module was delivered in English by another researcher who could not speak the learners' native language. The instructors delivering the modules were fully qualified, as confirmed in the post-assessment survey by learners. However, regarding the training delivered in English, learners expressed difficulties in understanding because of the use of technical terminology and their own limited English language proficiency.

In all of our conducted training sessions without exception, learners expressed their interest in learning about the coverage and approach of marine insurance such as Protection and Indemnity (P&I) and Hull and Machinery (H&M) insurance towards damages resulting from cyber attacks. This question could arise during the delivery of any module. In the MarCy programme, the relationship between marine insurance and cyber security is covered under the M8 Cyber Security Investments module. Although we believe that it is covered in the appropriate module, it would be beneficial for the instructors to have knowledge on the topic.

Apart from marine insurance matters, learners asked questions regarding contents covered in another module while discussing a module. Therefore, the instructor's general knowledge level of maritime cyber security is crucial in order to respond to such questions. According to the comments made by the learners in the post-assessment survey, the instructor's responses to the questions were well-received.

5.7.3 *Physical Resources*

The training sessions were organized as shown in Table 21, including online (live), on-site, and hybrid formats. This allowed the MarCy programme to be

verified for all three implementations, and it was observed that it could be successfully applied. Learners who participated online expressed that the live format, which provided opportunities for asking questions and engaging in discussions, increased their interest compared to video recordings. Some of the feedback received from the on-site training courses suggested that the training may be delivered online, but it was emphasized that training should be conducted in a live format.

Table 21. Modality, Meeting Platform, and Place

Partner	Modality	Meeting Platform	Venue
class society	on site	-	in house
maritime faculty	online (live)	Google Meet	-
student club	hybrid	Zoom	campus
training company	on site	–	hotel

During the training sessions conducted on Zoom and Google Meet platforms, both platforms worked reliably throughout the training duration. Although both instructors were not fully familiar with Google Meet, no issues were encountered. Only a few learners experienced initially sound-related problems because of their device or software settings, but these issues were quickly resolved.

For on-site training sessions, the instructor arrived at the training venue approximately 1.5 hours before the start time to test equipment. This proved to be very beneficial as it helped address some technical problems in advance. For instance, the instructor's laptop had only a Type-C interface, while the projectors had HDMI connections. As a result, a Type-C to HDMI converter was needed, which was not readily available in any of the training saloons. The instructor expected this issue and brought along a converter to address it.

Another issue encountered was related to microphones. The leaders of the Student Club that there would be no microphone or presentation remote for the hybrid training held on campus. Therefore, the instructor brought these devices. However, it was stated that there would be a microphone available for the presentation at the hotel where Training Company organized the training. It was observed prior to the training that there was a handheld microphone available, but it was deemed unsuitable for use during the long hours of the training. During the training organized by Training Company, some additional speakers provided training on different topics, and none of the invited speakers preferred to use handheld microphones. One of our partners had prepared a table microphone, which was more practical for this type of training. A headset or lapel microphone might be more convenient for such training sessions.

The projector, sound system, and other technical aspects were tested by partners or hotel staff before the training, and they were functional. However, during the training held at the hotel, it was discovered that a learner accidentally loosened the microphone receiver plug while plugging his mobile phone into the plug socket. As a result, the microphones stopped working. The issue was identified and resolved by the instructor. To prevent such problems in the future, having a technically qualified person present throughout the event would be beneficial. An additional laptop was kept ready during the training sessions. Apart from the internet, there were no issues with infrastructure such as ventilation and lighting. During the hybrid training, it was not possible to connect to the guest internet network on campus, so internet sharing was done through a mobile device to resolve the internet issue. Additionally, during our discussion with the leaders before the on-campus training, they mentioned occasional electrical problems. Therefore, an external battery for the laptop was brought.

5.8 *Conduct Training*

The purpose of this phase is to carry out the planned training [25]. The training sessions started with a 10-minute opening speech. The opening speech included an agenda, the mention that the training was part of the research activity, an overview of the modules to be covered, and an explanation of the purpose and content of the post-assessment survey. The post-assessment survey was distributed to the learners either before the opening speech. Some training sessions started late because of learners' tardiness. In the delayed sessions, the agenda inherently could not be followed, but all the sessions were concluded at the scheduled time. Positive feedback was received from learners regarding time management.

The leaders expressed that cyber security training should be repeated at least annually. However, they also emphasized that the frequency of repetition could be increased depending on updates to the training content. For instance, if there are new cyber security regulations issued by the IMO, flag states, or vetting societies, or if new cyber threats are identified, learners may need to receive immediate micro-trainings on these specific topics, while general and fixed subjects can be covered annually. The duration of the training will also vary based on this approach. For instance, it was mentioned that initial cyber security training may require over two days, while micro-training or refreshment training sessions could be shorter.

Table 22 provides information on the training durations, the number of modules delivered, and the time allocated per module. The indicated durations do not include breaks, lunch breaks, opening and closing speeches, or the post-assessment period. Only the net instruction time is shown, including discussions and questions. Approximately 20-25 minutes were allocated for each module. The MarCy programme recommends longer training durations per module, but it is mentioned that durations could be shortened based on feasibility and needs. In these organized training sessions, we needed to shorten the module durations to be able to test more modules and meet our partners' expectations for a wider range of content. This was achieved by particularly reducing the duration of the discussion sections.

Table 22. Duration per Module by Partners

Partner	Duration	Modules	Duration / Module
class society	3 hours	7	26 minutes
maritime faculty	2 hours	5	24 minutes
student club	2 hours	5	24 minutes
training company	1 hours 30 minutes	4	22 minutes

The MarCy programme also provides warnings about the refreshments offered during the training. During the training organized by Training Company, snacks and soft drinks were provided to the learners. The Class Society only offered soft drinks. Both organizations provided lunch for the learners but did not serve alcohol. There were no observed allergen warnings for the provided food and beverages. It would have been beneficial to include warnings considering potential allergies to various foods, such as dairy products. Additionally, learners' dietary preferences (e.g., vegan) should have been taken into consideration.

At the end of the training, as described in detail in Section 5.9.4, Yes-No questions were asked to gather learners' opinions about the training. Two of these questions were related to time management and questions asked. The questions and learners' Yes rates are provided in Table 23. The longest training was conducted with Class Society and took one day. However, half of the learners still found the training duration insufficient. Additionally, learners who believed they had the lowest chance of asking questions were once again from Class Society.

Table 23. Feedback from Learners regarding Duration

Question	Class Society	Maritime Faculty	Student Club	Training Company
D3. Did you have the chance to ask questions during / at the end of the training?	85%	93%	100%	100%
D6. Was the allocated duration of the training sufficient?	52%	87%	80%	71%

Due to time constraints during the training, some of the learners' questions could not be answered. Additionally, some learners expressed in the post-assessment survey that the training duration should be extended. Despite narrowing down the training curriculum and reducing the amount of discussion and case study exercises, it was observed that time was still insufficient. Based on the experience gained from the conducted training sessions and the feedback received from learners, no changes need to be made to the recommended durations for the modules in the MarCy programme. While the duration may vary depending on the module, it is still advised to allocate at least two hours per training module.

During the training sessions, we observed that some learners were unable to attend the entire training. Some arrived late, some left early, and some occasionally left the training session. We had discussed this issue with the leaders of partners during the pre-requisite survey. We learned that because of an occurred natural disaster, the academic calendar of Student Club had changed, and some learners had exams scheduled, preventing them from attending the entire training. It was also expected that learners working in the private sector needed to leave at times because of their job responsibilities. These circumstances, at least for some learners, hindered their ability to complete the entire training. The MarCy programme specifically advises company managers to have a substitute available during the training, and the fact that some learners were unable to follow the training continuously because of their job responsibilities confirmed the validity of this recommendation.

The learners' count was not very high, allowing for questions to be answered during the training. However, the exact number of learners for the training organized by Training Company was not known in advance. Therefore, a live Q&A was created on Mentimeter [23]. This way, learners could write their questions online from their laptops or mobile devices, and other learners could vote on these questions. The instructor could then answer these questions, starting from the ones with the highest votes, within the available time. This approach might have prevented potential time delays and ensured that the most popular questions were addressed, maximizing learner engagement.

The MarCy programme does not provide specific recommendations regarding the notification period for training sessions. Our partners informed the learners about the training approximately one week before the sessions. However, based on the feedback from learners, it became apparent that a one-week notification period may not be sufficient. It may be more effective to notify learners at least two weeks in advance of the training sessions to allow for better preparation and planning.

5.9 *Evaluation of the Training*

During the conducted sessions, each learner was given two multiple-choice exams, one before the training (Quiz) and one after the training (Test). This was done to measure the learners' knowledge level before and after the training and assess the effectiveness of the training on the topics covered. Approximately 10 minutes were allocated for the Quiz, and 15 minutes for the Test. Two questions were asked in the Quiz, and three questions in the Test for each module. The same two questions from the Quiz were also included in the Test. Table 24 displays the average score of learners in the Quiz (Q) and Test (T) results, presented on a scale of 100 points. The Success Rate (SR) in the table represents the percentage change in the score after the training. For example, the average score for Student Club in Module 1 Basic Cyber Security was 55 in the Quiz, and 90 in the Test. It was observed that the conducted training resulted in a 64% increase in the score.

Success Rate is criteria related to the effectiveness of the training and does not indicate whether learners are successful or unsuccessful. Especially in modules where learners have high Quiz scores, it is natural for the Test scores to be higher, resulting in a lower Success Rate. An example of this can be seen in the M1 Basic Cyber Security module given to Maritime Faculty. Conversely, the opposite is also possible. For instance, in the M5 Critical Deck Systems module given to Class Society, the Quiz score was 15, the Test score was 49, and the success rate was calculated as 146%. Although the training may be effective, it can be perceived that the level at which learners arrive at the end of the training is insufficient, requiring the need for the training to be repeated.

Table 24. Quiz and Test Results with Success Rate

Module	Class Society			Maritime Faculty			Student Club			Training Company		
	Q	T	SR	Q	T	SR	Q	T	SR	Q	T	SR
M1 Basic cyber security	63	97	54	70	80	14	55	90	64	-	-	-
M2 Advanced cyber security	67	91	36	57	71	25	75	90	20	-	-	-
M3 Regulatory requirements	54	83	54	43	58	35	45	60	33	73	87	19
M4 Vetting requirements	35	86	146	13	40	208	-	-	-	73	90	23
M5 Critical deck systems	15	49	227	-	-	-	40	47	18	29	44	51
M6 Critical engine systems	33	59	79	57	58	2	-	-	-	-	-	-
M8 Cyber security investments	-	-	-	-	-	-	-	-	-	31	77	148
M10 Cyber security management	35	80	129	-	-	-	-	-	-	-	-	-
M12 Autonomous ships	-	-	-	-	-	-	20	73	265	-	-	-
Average	43	78	81	48	61	27	47	72	53	51	75	47

Q: Quiz | T: Test | SR: Success Rate

5.9.1 *Score & Success Rate (SR) based Evaluation*

The average Quiz scores in the conducted training sessions range from 43 to 51, while the Test scores range from 61 to 78. Therefore, there is a Success Rate ranging from 27% to 81% after the conducted training sessions. The training sessions have resulted in an average score increase of 52%. It has been observed that all Test scores are higher than the Quiz scores. This indicates that the conducted modules provide benefits to the learners.

It is noticed that the MarCy programme does not provide any specific score recommendation for considering someone successful based on the exams conducted. A training designer should determine their own success criteria according to their needs. A general evaluation score or even a module-specific success score might be identified.

5.9.2 *Partner-based Evaluation*

In the training organized by Training Company, it was observed that the maritime company representatives attending the training obtained high scores in the Quizzes conducted for the M3 Regulatory Requirements and M4 Vetting Requirements modules. This is because both international regulations and vetting requirements are of great importance for a company's commercial operations. Therefore, those responsible need to closely monitor cyber security requirements as well. The Quiz scores also confirm this situation. However, as can be seen in Table 7, despite 74% of the learners having a deck background, they are not sufficiently familiar with the cyber security risks associated with deck systems. In the M8 Cyber Security Investments module, although the Quiz score was low (31), the Test score significantly increased to 77 after the training.

Class Society is the partner that has benefited the most from the training, with an 81% Success Rate in the overall evaluation. Additionally, their overall Test score is the highest among our partners, with 78. According to the Test scores, the modules where they showed the lowest success are M5 Critical Deck Systems and M6 Critical Engine Systems. Despite having low Quiz scores in the M4 Vetting Requirements and M10 Cyber Security Management modules (both are 35), their Test scores have reached 80 and over.

As seen in Table 7, 60% of the learners from the Student Club are students who are pursuing their education in non-maritime-related departments. Therefore, it is reasonable for the Quiz scores to be low in the maritime-related modules such as M3 Regulatory Requirements, M5 Critical Deck Systems, and M12 Autonomous Ships compared to the M1 Basic Cyber Security and M2 Advanced Cyber Security modules. It was observed that for the M5 Critical Deck Systems module, both the Test score and Success Rate were low. Despite having a low Quiz score in the M12 Autonomous Ships module (20), the Test score significantly increased to 73 after the training.

Learners of Maritime Faculty had the lowest overall Test score and Success Rate among our partners. It is the only partner with an average Test score below 70. As indicated in Table 21, all learners from Maritime Faculty participated in the training online. Conducting the training online may be a factor that contributed to the lower success rate. Our partner, Student Club, organized hybrid training, but only a couple of learners participated online. They also did not complete the post-assessment survey. Therefore, the exam results of the learners who participated online could not be compared.

5.9.3 *Learner Background and Module Relationship*

In Training Company, there were a sufficient number of learners with different backgrounds. Therefore, to analyze the impact of background, learners who participated in the training session organized by Training Company were examined.

Among the learners, 74% (n=23) had a deck background, while 26% (n=8) had backgrounds in naval engineering, computer science, maritime business management, and human resources. The achievements of learners with the deck background were compared to learners with other backgrounds. Because of the total number and diversity of backgrounds of learners with other backgrounds, they were grouped as "other". Table 25 presents the Quiz and Test scores, as well as the differences between Quiz-Test scores, based on modules.

It appears that learners with a deck background generally perform better in training. Observations show that, except for the M8 Cyber Security Investments module, learners with a deck background outperform those with other backgrounds in all modules. When examining the differences, it can be

observed that after the training, learners' scores become closer to each other, except for the M5 Critical Deck Systems module. This indicates that the training has brought learners with different backgrounds closer in terms of knowledge levels. Only in the M5 Critical Deck Systems module, the score difference has increased even further after the training.

Table 25. Exam Results by Background

Code	Module	Exam	Deck	Other	Difference
M3	Regulatory	Quiz	78	56	22
	Requirements	Test	90	83	7
M4	Vetting	Quiz	83	44	39
	Requirements	Test	93	83	10
M5	Critical	Quiz	35	13	22
	Deck Systems	Test	52	21	31
M8	Cyber security	Quiz	28	38	-10
	Investments	Test	77	79	-2
	Average	Quiz	56	38	18
		Test	78	65	13

The M5 Critical Deck Systems module differs from other delivered training modules in that it has more technical content. It covers the cyber risks of components such as GNSS, Automatic Identification System (AIS), ECDIS, RAdio Detection And Ranging (RADAR), and Very-Small-Aperture Terminal (VSAT). Therefore, learners need some technical knowledge about the functions of these components, their importance, and interdependencies before the training. Learners with a deck background are more familiar with this technical knowledge compared to learners from other fields because of their education and experience. These findings demonstrate that the learner's background is important, particularly for modules with technical content.

5.9.4 *Module-based Evaluation*

M1 Basic Cyber Security and M2 Advanced Cyber Security modules have acceptable Quiz scores of 55 and above. The M1 Basic Cyber Security module covers fundamental knowledge and is designed considering ratings that may have lower educational levels and serve on ships. As seen in Table 7, most our learners have a bachelor's degree or above or are currently pursuing undergraduate studies. Therefore, it is likely that their computer literacy level is higher when compared to ratings. Hence, the training should not be made more challenging based solely on Quiz scores. After applying the module to ratings, the decision to increase or maintain the difficulty level of the training can be made.

The M3 Regulatory Requirements module was delivered commonly to all partners. In the training organized by Training Company, it is observed that company representatives were already familiar with IMO regulations related to cyber security even before the training. When comparing the Test scores of professionals (learners of Class Society and Training Company) with students (learners of Maritime Faculty and Student Club), it can be seen that professionals have higher scores. The Student Club and Maritime Faculty took the M3 Regulatory Requirements module, which is the only common module related to maritime. It is observed that the Quiz, Test, and Success Rates of both groups of learners (undergraduate students) are very close.

It is observed that company representatives participating in the training conducted with Training Company have the highest Quiz score for the M4 Vetting Requirements module. Students usually encounter vetting programs when they start working in the industry, while Class Society employees do not. However, there are non-technical requirements in vetting programs that do not rely on cyber security-related technical knowledge. Therefore, both Class Society and Maritime Faculty have significantly increased success rates after the training.

After the Quiz, learners raised objections to the questions in the M4 Vetting Requirements module. Some company representatives argued that they did not need to know about the RightShip requirements of dry bulk vessel operators or cyber security requirements in Ship Inspection Reports (SIRE), Chemical Distribution Institute (CDI), and Tanker Management and Self Assessment (TMSA) of tanker operators. The learners were justified in their objections. In fact, the MarCy programme suggests that the M4 Vetting Requirements module should be designed based on the learners' specific vetting program needs. However, it was not possible to group the learners accordingly in the conducted training, so the cyber security requirements of all vetting programs were examined in our training sessions. The questions in the Quiz and Test were prepared by considering the fundamental aspects of cyber security. For instance, including component passwords or personal information of crew members in the Cyber Security Plan (CSP), accessible by all ship crew, including third parties such as representatives of class societies, would be incorrect. No vetting program requires such information to be included in a CSP. In the exams, we asked questions regarding the accuracy of such aspects based on vetting programs. This allowed for awareness to be raised among learners about general aspects of cyber security.

The M5 Critical Deck Systems and M6 Critical Engine Systems modules focus on technical topics. All the learners were not familiar with the systems discussed in these modules. This was observed as a barrier to fully understanding training modules because they were trying to learn about the cyber security risks of systems they were not sufficiently familiar with. Although the importance of learners' backgrounds were highlighted in Section 5.9.3, it can be seen that achieving success with a single short-term training is challenging. As aforementioned, the MarCy programme suggests allocating two hours at least for each of these modules.

M8 Cyber Security Investments, M10 Cyber Security Management, and M12 Autonomous Ships modules are not heavily focused on technical knowledge. Although the Quiz scores may have been low, it has been confirmed that understanding improved based on the higher scores achieved in the Tests conducted after the training.

The MarCy programme suggests introducing learners to the critical systems onboard and then starting the modules of the M5 Critical Deck Systems, M6 Critical Engine Systems, and M7 Other Critical Systems modules. However, due to time constraints, the mentioned target systems could not be covered. Additionally, during the training sessions, it was

observed that university students, in particular, may not be familiar with maritime notions such as the ISM Code and ISPS Code. The MarCy programme expected this issue and recommended including maritime notions in the curriculum, with the expectation of explaining them at the beginning of the relevant modules. However, due to time limitations, these notions could not be provided to the learners during the conducted training sessions, as described in detail in Section 5.5. The absence of these notions did not pose any problem in the training of the company representatives.

5.9.5 *Feedback based Evaluation*

For each module, learners were asked score-based questions and yes-no questions for the overall evaluation of the training. Additionally, open-ended questions were used to gather general feedback. The module-specific questions asked are listed below, and the scores provided by the learners are shown in Table 26 and Table 27. The comments made by learners in response to the open-ended questions can be found in relevant previous sections.

- Q1. How satisfied were you with the overall quality of the module?
- Q2. Was the module presented in an engaging and interactive manner?
- Q3. Did you find the module relevant to your job responsibilities? If you are a student, you can consider potential responsibilities after graduation while answering.
- Q4. Did you find the module material easy to understand?

According to the scores given by the learners for Q1, the overall quality of the modules ranges from 4.2 to 4.8. This score range indicates that learners are satisfied with the overall quality of the training modules. The scores for Q2 range from 4.1 to 4.8. Based on the learners' ratings, the modules were delivered engagingly and interactively. Detailed explanations regarding Q3 are provided in Section 5.3. Regarding Q4, which is related to the training materials, the scores range from 4.1 to 4.9, indicating overall success. However, learners from the Maritime Faculty rated the M1 Basic Cyber Security module with a score of 3.7 for this question. The learners of other two partners gave scores of 4.5 and 4.8 for the M1 module. The same training materials were used in all our partners. The M1 Basic Cyber Security module differs only in terms of the instructor aspect for the Maritime Faculty. As explained in Section 5.7.2, the module was presented in English upon the request of the course coordinator, but only for the Maritime Faculty and only for the M1 module. The presentation language may have influenced the lower score.

The Yes-No questions were asked to gather learners' overall opinions on the conducted training and the percentage of Yes answers is provided in Table 28. Except for the students at the Maritime Faculty partner, almost all learners believe that they need more training on maritime cyber security. In most learners' opinion, their organizations or educational institutions should allocate more time and resources to cyber security topics. Detailed explanations and corrections for D3, D5, and D6 are provided in Section 5.8.

Table 26. Feedback from Learners on Modules 1-4

	M1			M2			M3				M4		
	MF	SC	CS	MF	SC	CS	MF	TC	SC	CS	MF	TC	CS
Q1	4.4	4.5	4.2	4.5	4.7	4.5	4.3	4.6	4.5	4.5	4.3	4.6	4.2
Q2	4.3	4.2	4.2	4.4	4.6	4.5	4.3	4.7	4.3	4.3	4.3	4.7	4.1
Q3	4.3	4.2	4.1	4.1	4.4	4.0	4.2	4.8	3.3	4.3	4.4	4.6	3.6
Q4	3.7	4.8	4.5	4.3	4.9	4.3	4.1	4.8	4.4	4.4	4.2	4.8	4.1

MF: Maritime Faculty | TC: Training Company | SC: Student Club | CS: Class Society
5 is the highest score

Table 27. Feedback from Learners on Modules 5-12

	M5			M6		M8	M10	M12
	TC	SC	CS	MF	CS	TC	CS	SC
Q1	4.8	4.5	4.4	4.7	4.3	4.7	4.4	4.7
Q2	4.8	4.5	4.2	4.3	4.4	4.7	4.5	4.7
Q3	4.7	3.7	4.0	4.5	4.2	4.5	4.1	4.6
Q4	4.9	4.4	4.4	4.4	4.3	4.8	4.5	4.9

Table 28. Questions in the Post-Assessment Survey and the Rates of Yes

Question	Class Society	Maritime Faculty	Student Club	Training Company
D1. Did the training help you understand the importance of cyber security for the maritime sector?	100%	100%	100%	100%
D2. Did the training help you identify specific cyber risks in the maritime sector?	100%	100%	100%	100%
D3. Did you have the chance to ask questions during / at the end of the training?	85%	93%	100%	100%
D4. Do you believe you may require further maritime cyber security training?	95%	80%	100%	94%
D5. Do you believe the notification period of the training sufficient?	86%	87%	70%	81%
D6. Was the allocated duration of the training sufficient?	52%	87%	80%	71%
D7. The presentation was prepared in English, but the delivery was done in Turkish (native language). Was this approach suitable for you?	81%	100%	100%	97%
D8. Did the training meet your needs?	90%	100%	100%	84%
D9. Do you believe your company needs to allocate more time and resources to cyber security issues? (If you are a student, do you believe your university needs to allocate more time and resources to cyber security education?)	86%	87%	100%	100%

6 CONCLUSION

The maritime industry is increasingly vulnerable to cyber attacks because of the advancement of digital technologies. Technical measures alone are not sufficient to counter these cyber threats; the human element must also be considered. Therefore, the awareness of employees towards cyber risks should be increased through regularly conducted comprehensive training programs.

In our original study, we developed an approach called the MarCy training programme, following scientific methods, which enables the design of cyber security training for professionals working in the maritime domain. This programme offers 11 elective modules that can be used for the training of office employees and seafarers working in ship operators. However, the programme is not limited to the training of seafarers or office employees only; it also caters to different dimensions of the maritime domain.

The study aimed to evaluate the effectiveness of the MarCy training programme through four training sessions involving a total of 79 students and professionals. The programme was improved based on evaluations and feedback from the learners, resulting in an enhanced approach to maritime cyber security training. Two pre-requisite surveys were administered to understand the training needs and expectations of both partners' leaders and invitees. Meetings were held with leaders to gather their perspectives, while an online survey was shared with invitees. 35 invitees completed the pre-requisite survey, including 19 undergraduate students from various departments in the Student Club and 19 professionals from maritime companies invited by the Training Company. The training sessions were planned based on the analysis of training needs and expectations, and training materials and post-assessment surveys were prepared. Post-assessment surveys were conducted during the training sessions to evaluate their effectiveness. The post-assessment survey was completed by a total of 79 learners, comprising 54 employees and 25 students. During the training sessions, learners completed the post-assessment surveys, participated in module evaluations, training evaluations, and took two exams. The observations, evaluations, feedback, and exam results were analyzed to assess the training sessions. The MarCy programme was refined based on the findings, observations, and feedback obtained.

In addition to our original study, this study provides cyber security training recommendations for technical staff working in class societies. Furthermore, a new module called M12 Autonomous Ships was designed. Recommendations were made for the objectives, learning outcomes, curriculum, training material, and duration of the training for the module, as well. This study also includes the corrections and improvements of certain issues in the MarCy programme. The responsibility list of office employees working in ship operators was revised, and accordingly, the responsibility-module mapping was updated. The original study did not consider the passing score for the final exam and the notification period for potential learners to be invited for training. The proposed frequency of the training was insufficient, as well. Improvements were made regarding these mentioned aspects in this study.

Credited organizations in the maritime sector argue that cyber security training should be designed considering the roles and responsibilities of the learners. The MarCy programme was designed in line with this recommendation, and this research confirmed the validity of the proposed recommendations. This study verifies that the training needs of organizations and learning groups in the maritime industry regarding maritime cyber security differ, emphasizing the importance of tailoring the training programs to meet these specific needs. Additionally, it confirms that the MarCy programme can be used for the training of students, professionals working in ship operators, and technical personnel in class societies. Moreover, through the recently developed M12 Autonomous Ships module, it was confirmed that a new training module can be created using the MarCy programme. Another verification in this study is that the MarCy programme can be used for hybrid, online, and on-site training programs.

It was observed that background knowledge is crucial in understanding the cyber risks of critical ship systems. Therefore, when forming learning groups, it is beneficial to group individuals with close knowledge levels. Otherwise, the curriculum should be planned considering learners with lower knowledge levels so that at least a basic level of knowledge can be established for all learners. However, this approach may lead to longer and less engaging training sessions for learners with more advanced knowledge levels. Our study has shown that regardless of the initial differences in learners' knowledge levels in cyber security, they converged towards each other after the training.

Issues were encountered during the digital delivery of training materials. Therefore, it was understood that sharing hard copies with the learners before the training is essential. Despite all measures, problems related to physical resources were observed. Therefore, especially in on-site training programs, it was determined that having a technically qualified staff member familiar with the setup and use of systems would be beneficial.

Our study demonstrated that individuals are aware of what they know and don't know about maritime cyber security. It was found that at least 31% of maritime companies have previously experienced cyber attacks, while only 25% of office employees have received maritime cyber security training. Most company employees were aware of the cyber security regulations in force by the IMO.

Although training can be conducted online, it was understood that even in online settings, live sessions are necessary for learners to receive answers to their questions and engage in discussions. Among instructional strategies, case study method is particularly preferred by learners. However, the number of documented cyber incidents in the maritime industry with detailed is relatively low in the literature. Therefore, developing a platform that lists documented cyber attacks supported by class societies, insurance companies, and flag states would

be beneficial for enhancing the resilience of the entire maritime industry against cyber risks.

In future studies, the training programs of other dimensions of the maritime domain, such as naval forces and maritime authorities, can be developed and evaluated using the MarCy programme. Online and on-site training programs can be tested for their effectiveness by forming equivalent learner groups. Although the relationship between cyber security and background was briefly addressed in this study, further research can be conducted to explore this relationship in more detail.

Based on the exam results before and after the training, this study demonstrates that the MarCy programme increased learners' scores by 27% to 81%. According to the learners' opinions, it is emphasized that a mandatory course should be developed by following the MarCy programme to address the cyber security training needs of cadets.

FUNDING

This paper has received funding from the Research Council of Norway through the Maritime Cyber Resilience (MarCy, project number 295077) project and the SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS, project number 310105). 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.

ACKNOWLEDGE

We would like to express our sincere gratitude to our partners for their collaboration towards improving the MarCy training programme.

REFERENCES

[1] Sauli Ahvenjarvi, Ireneusz Czarnowski, and John Mogensen. Addressing Cyber Security in Maritime Education and Training (CYMET). Ed. by Gamal Ahmed Mohamed Ghalwash and Aykut Olcer. Tokyo, Japan, 2019. URL: http://archive.iamu-edu.org/download/final-report-of-research-project-fy2018/?wpdmdl=6691 (visited on 09/29/2022).

[2] BIMCO and ICS. Seafarer workforce report. Scotland, UK, 2021. URL: https://shop.witherbys.com/seafarer-workforce-report/ (visited on 05/21/2023).

[3] BIMCO et al. The guidelines on cyber security onboard ships. 2020. URL: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf (visited on 03/21/2022).

[4] Victor Bolbot et al. "Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis". In: International Journal of Critical Infrastructure Protection 39 (2022), p. 100571. ISSN: 18745482. DOI: 10.1016/j.ijcip.2022.100571.

[5] C4ADS. Above us only stars. 2019. URL: https : / / c4ads . org / wp - content / uploads / 2022 / 05 /AboveUsOnlyStars-Report.pdf (visited on 04/15/2023).

[6] Cambridge. Attitude. 2023. URL: https : / / dictionary . cambridge . org / dictionary / english /attitude (visited on 05/25/2023).

[7] Monica Canepa et al. "Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain". In: 15th International Technology, Education and Development Conference (INTED 2021). Ed. by Luis Gómez Chova, Agustín López Martínez, and Ignacio Candel Torres. Valencia, Spain: IATED Academy, 2021, pp. 3489–3499. ISBN: 978-84-09-27666-0. DOI: 10.21125/inted.2021.0726.

[8] Nabin Chowdhury and Vasileios Gkioulos. "A personalized learning theory-based cyber-security training exercise". In: International Journal of Information Security (2023), pp. 1–16. DOI: 10.1007/s10207-023-00704-z.

[9] Citavi. Reference management and knowledge organization. URL: https://citavi.com/en (visited on 06/20/2023).

[10] Cyber-MAR. The project. 2019. URL: https://www.cyber-mar.eu/ (visited on 05/20/2023).

[11] Mazlitdinova Dilnoza et al. "Modular training system as a factor of improving educational process". In: International Journal of Innovative Technology and Exploring Engineering (IJITEE) 9.1 (2019), pp. 3160–3166. DOI: 10.35940/ijitee.A9152.119119.

[12] DNV. DNV-CG-0264 Autonomous and remotely operated ships. 2001. URL: https : / / www . dnv . com /maritime/autonomous-remotely-operated-ships/class-guideline.html (visited on 05/23/2023).

[13] DSCA. Implementation guide for cyber security on vessels. 2020. URL: https://dcsa.org/wp-content/uploads/2020/03/DCSA-Implementation-Guideline-for-BIMCO-Compliant-Cyber-Security-on-Vessels-v1.0.pdf (visited on 10/22/2022).

[14] Erlend Erstad et al. "A human-centred design approach for the development and conducting of maritime cyber resilience training". In: WMU Journal of Maritime Affairs 22.2 (2023), pp. 241–266. DOI: 10.1007/s13437-023-00304-7.

[15] Finferries. Finferries' Falco world's first fully autonomous ferry. 2018. URL: https://www.finferries.fi/en/news/press-releases/finferries-falco-worlds-first-fully-autonomous-ferry.html (visited on 05/24/2023).

[16] Sarah French. The benefits challenges of modular higher education curricula. Australia, 2015. URL: https://eric.ed.gov/?id=ED573806 (visited on 05/21/2023).

[17] IMO. Autonomous shipping. URL: https : / / www . imo . org / en / MediaCentre / HotTopics / Pages /Autonomous-shipping.aspx (visited on 05/24/2023).

[18] IMO. HTW 8/15/1 Any other business: Necessity of developing relevant provisions concerning cybersecurity related training for seafarers. London, UK, 2021.

[19] IMO. Resolution MSC.428(98) Maritime cyber risk management in Safety Management Systems. London, UK, 2017.

[20] Georgios Kavallieratos and Sokratis Katsikas. "Managing cyber security risks of the cyber-enabled Ship". In: Journal of Marine Science and Engineering 8.10 (2020), p. 768. DOI: 10.3390/jmse8100768.

[21] Paloma de La Vallée et al. "Sector-specific training - A federated maritime scenario". In: Multimedia Communications, Services and Security. Ed. by Andrzej Dziech, Wim Mees, and Marcin Niemiec. Vol. 1689. Communications in Computer and Information Science. Cham: Springer International Publishing, 2022, pp. 21–35. ISBN: 978-3-031-20214-8. DOI: 10.1007/978-3-031-20215-53.

[22] Lloyd's Register. ShipRight procedure assignment for cyber descriptive notes for autonomous & remote access ships. 2017. URL: https : / / maritime . lr . org / l / 941163 / 2021 - 12 - 09 / 2pwb2 / 941163 /1639061961zcaozhcz/mo_cyber_enabled_ships_shipright_procedure_v2.0_201712.pdf (visited on 05/24/2023).

[23] Mentimeter. Live Q&A. URL: https://www.mentimeter.com/features/live-questions-and-answers (visited on 05/22/2023).

[24] Moodle. Moodle Learning Management System (LMS). 2023. URL: https://moodle.com/solutions/lms/(visited on 06/23/2023).
[25] Nadler and Leonard. Designing training programs: The Critical Events Model. US: Addison-Wesley Publishing, 1982.
[26] NTNU. Autonomous all-electric passanger ferries for urban water transport (Autoferry). URL: https://www.ntnu.edu/autoferry (visited on 05/24/2023).
[27] NTNU. Autosea. URL: https://www.ntnu.edu/autosea (visited on 05/24/2023).
[28] OCIMF. Ship Inspection Report (SIRE) Programme. London, UK, 2018. URL: https : / / www . ocimf .org / document - libary / 287 - sire - vessel - inspection - questionnaire - viq - ver - 7007 -questionnaire/file (visited on 10/25/2022).
[29] Aybars Oruc. "Ethical considerations in maritime cybersecurity research". In: TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation 16.2 (2022), pp. 309–318. DOI: 10.12716/1001.16.02.14.
[30] Aybars Oruc, Nabin Chowdhury, and Vasileios Gkioulos. "A modular cyber security training programme for the maritime domain". In: International Journal of Information Security (2024). DOI: 10.1007/s10207-023-00799-4.
[31] Aybars Oruc, Nabin Chowdhury, and Vasileios Gkioulos. Pre-requisite survey for invitees. 2023. URL: https://cyberonboard.com/files/Pre-Requisite_Survey_(Invitee).pdf (visited on 07/06/2023).
[32] Aybars Oruc, Nabin Chowdhury, and Vasileios Gkioulos. Pre-requisite survey for leaders. 2023. URL: https://cyberonboard.com/files/Pre-Requisite_Survey_(Leader).pdf (visited on 07/06/2023).
[33] Aybars Oruc, Nabin Chowdhury, and Vasileios Gkioulos. Specified post-assessment survey for the Class Society. 2023. URL: https://cyberonboard.com/files/Post-Assessment_Survey.pdf (visited on 07/06/2023).
[34]Oxford. Knowledge. 2023. URL: https : / / www . oxfordlearnersdictionaries . com / definition /english/knowledge?q=knowledge (visited on 05/25/2023).
[35] Oxford. Skill. 2023. URL: https://www.oxfordlearnersdictionaries.com/definition/english/skill?q=skill (visited on 05/25/2023).
[36] Jaime Pancorbo Crespo, Luis Guerrero Gomez, and Javier Gonzalo Arias. "Autonomous shipping and cybersecurity". In: Ciencia y tecnología de buques 13.25 (2019), pp. 19–26. ISSN: 1909-8642. DOI: 10.25043/19098642.185.
[37] Georgios Potamos et al. "Building maritime cybersecurity capacity against ransomware attacks". In: Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media. Ed. by Cyril Onwubiko et al. Springer Proceedings in Complexity. Singapore: Springer Nature Singapore, 2023, pp. 87–101. ISBN: 978-981-19-6413-8. DOI: 10.1007/978-981-19-6414-56.
[38] Sanoma Group. itsLearning global. 2023. URL: https://itslearning.com/global/ (visited on 06/23/2023).
[39] Sanjeev Singh et al. "Improving outcomes and reducing costs by modular training in infection control in a resource-limited setting". In: International Journal for Quality in Health Care 24.6 (2012), pp. 641–648. DOI: 10.1093/intqhc/mzs059.
[40] Gregory J. Skulmoski, Francis T. Hartman, and Jennifer Krahn. "The Delphi method for graduate research". In: Journal of Information Technology Education 6.1 (2007), pp. 1–21. URL: https://www.learntechlib.org/p/111405/ (visited on 05/21/2023).
[41] Hasan Mahbub Tusher et al. "Cyber security risk assessment in autonomous shipping". In: Maritime Economics & Logistics (2022). DOI: 10.1057/s41278-022-00214-0.
[42] UNCTAD. Review of maritime transport 2022. New York, USA, 2022. URL: https : / / unctad . org /publication/review-maritime-transport-2022 (visited on 05/21/2023).
[43] University of Oslo. Nettskjema. URL: https://nettskjema.no/?lang=en (visited on 06/20/2023).
[44] USCG. CVC-WI-27(2) Vessel cyber risk management work instruction. Washington, USA, 2022. URL: https://www.dco.uscg.mil/Portals/9/CVC-WI-27%282%29.pdf (visited on 06/13/2023).
[45] Witherbys, BIMCO, and ICS. Cyber security workbook for on board ship use. 2022.
[46] Yara International. Yara Birkeland. URL: https://www.yara.com/news-and-media/media-library/press-kits/yara-birkeland-press-kit/ (visited on 05/24/2023).

.