ASSESSING THE EFFECTIVENESS OF CYBERSECURITY TRAINING AND RAISING AWARENESS WITHIN THE MARITIME DOMAIN

M. Canepa, F. Ballini, D. Dalaklis, S. Vakili

World Maritime University (SWEDEN)

Abstract

In recent years, the use of digital means is rapidly expanding throughout the whole world and the maritime industry is not an exception; dealing effectively with the issue of “Cyber Security” should be a high priority issue for the numerous maritime stakeholders. It is also useful to point out that the maritime sector still maintains its importance for today’s global economy: acting as the backbone of world trade, approximately 80-90% of goods and raw materials are served nowadays by the international shipping industry. Additionally, the so-called "digitalization phenomenon" is rapidly expanding in all sectors of the economy, including the maritime one; both onboard ships and in ports, Information Technology (IT) applications systems are numerous, and very often designed without taking into account the growing cyber risks. The Cyber-MAR Project is focused on hyper-realistic simulation and emulation of maritime systems (e.g. Supply Chain) and aims to create a federated Cyber Range (CR Cyber-MAR) which will include various platforms and interconnected systems onboard a ship or on land, in order to facilitate a real-time simulation of cyber-attacks and relevant malicious attempts. Cutting a long way short, CR Cyber-MAR will be an integral part of an ambitious IT security training offer, aimed at target groups with different levels of experience and technical skills available. The analysis at hand will initially deliver a literature review in relation to education and training on cybersecurity, with a very dedicated focus on the maritime domain. Then, a discussion of the position of the International Maritime Organization on the wider topic of maritime cybersecurity will be taking place. Afterward, the impact of a training session affiliated with the Project under discussion will be provided. A conclusion clearly standing out is that the vast majority of participants confirmed an improvement in their cybersecurity skills, as well as an increased level of awareness towards cyber threats.

Keywords: Maritime cyber security, Training and awareness-raising, Cyber-MAR Project

1. INTRODUCTION

In recent years, the use of digital means is rapidly expanding throughout the whole world and the maritime industry is not an exception; shipping companies are relying on a much-extended number of computers and Information Technology (IT) applications to effectively support their business activities. Increasing interconnection of computer base with maritime section increase efficiency and productivity within the cluster. However, this has increased the risk of potential cyber-attacks that at a minimum could disrupt normal business activities [1].

At the same time, the safe conduct of navigation is heavily supported by a significant number of interconnected electronic systems and various digital means [1]. Number of incidents have been occurred in maritime cluster such as effect of Electronic Chart Display Information System (ECDIS), which leads to severe financial consequences [2], as well as threat safety and security of vessels.

Dealing “Cybersecurity” as a new emerging phenomenon becomes as one of the highest priorities in the maritime cluster. As a result, professionals with well training and education will be needed to cover whatever gap is created by the advance of the so-called “digitalization phenomenon” and the associated cyber risks. This in turn is indicating a need for continuous training activities to add more resources in the workforce pool, who should be equipped with the “right” skills and fully updated with the newest IT trends.

In the new era of digitalization, the Resolution MSC.428 (98) adopted by the International Maritime Organization (IMO) to addresses cyber risks in the maritime industry. The IMO resolution effectively addresses cyber risks as a part of safety management systems within the ISM Code and administrators are to ensure their existing safety management systems appropriately address cyber risks by their 2021 annual verification.

Furthermore, the SMS should include instructions and procedures to be sure that company’s instruction and procedures are safe and protecting the environmental in accordance of Administration

requirements. The SMS has to consider cyber risk and that may arising from the use of IT onboard, and consider and apply the related guidelines.

2. METHODOLOGY

This paper aims to illustrate and analyse the main challenges relating to maritime cybersecurity training and the use of the Cyber-range as solution. For investigating possible solutions, the CyberMAR project [3] will be presented, as it will adopt a federated Cyber Range solution as part of a cybersecurity training platform focused on the peculiarities of the maritime sector. The implemented methodology is based on a qualitative approach: a literature review, an analysis of the target groups that will be involved in the training. Furthermore a a quantitative approach has been adopted for analyzing the results of the first implemented LMS training.

3. GENERALITIES

The maritime sector is under an on-going process of digitalization in all aspects of operation. Ships are becoming strictly integrated with shore-side operations since digital communication and data links are used to conduct business, manage operations, and control equipment/services. Very often critical systems essential to the safety of navigation, power and cargo management are connected to the Internet to perform a variety of functions and awareness of risks is not so widespread [4] [9] [10].

A reasonable defensive strategy to cope with evolving cyber threats needs increasing awareness and then exploit that awareness to implement defence strategies and activate early risk mitigation measures. Extensive dedicated training is a solid basis to achieve this objective.[8]

Insufficient knowledge of security procedures and the lack of security awareness is a rather common problem that is further exacerbated by quick changing of technological scenarios. Clearly a training program is crucial for security, but in order to be effective it must be well tailored to the trainee's needs, also enabling them to ongoing adaptation of his/her capabilities as risk situation to be faced continuously evolves. All the studies show that reaching a high-order of thinking and understanding of the risk is quite important and of great importance in the cyber-security field. A rather complete overview of strategies, training methodology and its evolution and course assessment may be found in [13] to [19]

As noted earlier, ships are becoming more and more integrated with shore-side operations because digital communication is being more and more used to carry business, manage operations, and stay in connection with head office. Furthermore, critical ship systems essential to the safety of navigation, power and cargo management have been increasingly digitalized and connected to the Internet to perform a wide variety of legitimate functions (e.g., updates, versioning upgrades, remote maintenance, voyage or ship performance monitoring from ashore) [4].

As people are generally considered the weakest link in a computer system, professional training is now becoming a necessity, not only for raising the users' awareness but also for training the technical staff to operate the various protection mechanisms that must be acquired (e.g., cryptographic protocols, intrusion detection/prevention systems, machine learning and artificially intelligent modules, digital forensics, etc.). Gartner estimates that the global cyber-security awareness and training market will worth around USD 1.5 billion by 2021 [4]

The rapid technological advancements and the digital evolution of companied is likely to increase the number of attacks and their effectiveness against tangible and intangible assets in may organizations and in the maritime ones of course .

Cyber threats targets vulnerabilities of the systems exist since a lot of time but are increasing in sophistication and potential danger. Protective barriers either in the form of technical protection or human awareness are set forward to prevent attack from impacting the system network components and cause negative consequences.

In this context cybersecurity education and training are becoming more and more relevant, as the only way in which such cyber breaches can be prevented and handled adequately. Following this reasoning a proposal for training education and assessment is being proposed, it is based on many achievement described by current practices and the basis is in part derived from CyTrONE (Cybersecurity Training and Operation Network Environment), a cybersecurity training framework that aims to facilitate training activities by providing an open-source framework that automates the training content generation and environment setup tasks.[5]

It is necessary to remark that unfortunately the awareness of employees and their skills do not increase at the same pace of cyber threats.[6] so that to protect assets and minimize consequences of attacks, maritime organizations need to train appropriately their employees on the basis of their role

and level of responsibility. Effectiveness of proper training requires access to training scenarios that that are able to simulate (in time and modes) situations that may occur in the respective organization and link these organizations together to create a very comprehensive and realistic scenario to be used for real time training[6].
The global cybersecurity awareness and training market, according to Gartner estimates, will be worth approximately $ 1.5 billion by 2021 [20].
Training requires proper framework than needs to be quickly configured, the key is automating the training content generation and environment setup tasks, model accurately the scenarios, create proper training scenarios, change situation on line, assess and review trainees. For a realistic training, trainees need also communicate with staff members, similarly to what would be required in the case of a real cyber-attack, for instance in order to report the issue to management, to request assistance from a cybersecurity specialized company.
Proposed training will be generally targeted to:

- On board personnel
- Ground personnel including the ones that support operations of the ship

As the trainee accomplishes his/her basic evaluation tasks, the training program starts involving more advanced features that demand a higher level of understanding. The overall method is integrated in a cyber-ranges platform.[4]
Proposed training programs range from introductory short basic courses to highly specialized certifications for security experts. This means offering traditional in-class teaching, on-line training platforms and virtual labs, in short what we are proposing is based on cyber-ranges frameworks that mirror an actual system and give hands-on experience to the trainee under realistic operational conditions. Pedagogical principles are taken into account as well. [4] General surveys concerning cyber-security exercises are reported in [8-10]
The training environments used for cybersecurity training are typically known as cyber ranges where the trainees will access to a network environment in which they can practice and improve their skills. This environment may contain traces of cyber-attacks, for use in forensics training, but could also be subjected to live attacks by white-hat hackers, for use in defense and even attack training.
Cyber Ranges provide a multipurpose virtual environment where organizations can test critical capabilities and reveal how effectively they integrate people, processes, and technology to protect their strategic information, services, and assets. Students can reach competence in cyber-security only via hands-on learning with virtual labs led by an instructor [4]. Therefore, the proposed training program will incorporate a series of dedicated content, interaction, pedagogical framework, and important virtualized exercises for hands-on interplay.
Starting from these considerations a Cyber range training [8] is proposed since in our opini9ons it looks very appropriate for application in maritime environment, in fact:

- Is generally applicable to many type of a organizations ;
- Can be modelled (enough easily) to generate training scenarios customized on type , work flow and assets of a maritime organization (ii)
- Is scalable to fit evolution and organizational changes of organizations (what can cause new vulnerabilities)
- Is upgradable to face new challenges

Realistic simulations for Cyber Range training programs are based on a model that is created on the basis of recognized Threats, Security Controls while monitoring is employed to measure the performance of the trainees.

3.1 Cyber range Model

The Cyber-Range sub-model will be developed to provide essential information for the specification and implementation of the Cyber-Range training programs. [6] and [8] The proposed model to Cyber-Range training will be based on the concept of the construction of a Security Assurance Model that permit a rather exhaustive representation of the port organizations, their assets and their relations, and, ultimately, their security level. It will be based on a number of sub-model each one characterizing a particular topic/activity/scenario. Software simulation, and diverse training capabilities, are what has drawn so much attention to Cyber Ranges and what makes this environment easily customized for different needs.[8]
The potential of model-driven Cyber-Range training that will be implemented is that is applicable to any type of a system, is able to represent the actual assets of organizations and generate training scenarios based on them . It provides scalability and adaptability, it makes relatively easy customizations, taking into account new vulnerabilities [6]

The model will provide a formalized description of the assets of the organizations, their mutual relationships and their associated threats, the likely sequence of events that may lead to the appearance of these threats, alongside the responsible actor; the actions that trainees are expected to take against these attacks and the tools that may be used for this purpose
These targets regard the preparedness and effectiveness level that the trainees targeted by a Cyber-Range training program are expected to achieve and how these levels may be measured in different stages of the delivery of the program; and eventually information on how the system can simulate and emulate the components necessary for its implementation.
Cyber-Range sub-models will permits to build custom training scenarios for cyber-attacks allowing trainees to learn how to effectively and systematically utilize different security tools; learning the procedure for various types of actions and security processes[6].
This approach will allow to provide automated means for generation of tailored Cyber-Range training programs that align with the organizations composition and security requirements.[5]
The core of the defined security assurance model are the organizations assets (i.e., anything is of value for the organization), as well as the interplay between threats, vulnerabilities, security properties and security controls.
Training scenarios will be generated within cyber range considering the systems assets, threats, security properties and security controls. For example, if a certain system isn't prone to phishing attacks, then the cyber range dedicated will not generate a phishing training scenario.

3.1.1 Cyber-Range sub model

The Cyber-Range sub-models will be implemented to accommodate a detailed and comprehensive representation of simulation environments and its components in order to support automatic generation of the simulation demands of the training program. Since the overall security level is only as strong as the weakest link it will generate a model aimed to holistically assess all dimensions of security in order to minimize the likelihood that a given threat takes advantage of the weakest link. [6]
The sub-models will enable the systematic representation of the port organizations , their assets and their mutual relations and its security . A very critical point of proposed training that will be organized is teaching appropriately and monitoring the actions that trainees are expected to take against attacks and how they use tools that may be used for this purpose; in this way it will be assessed along different stages of the training process the preparedness and effectiveness level that the trainees will achieve under the Cyber-Range training program .
To create different levels of difficulty and of execution steps of a training scenario, the cyber-range sub model will be configured taking into account information about the working role of the trainee. [6]
Additionally the model will include the sequence of events that lead to the manifestation of the threats , they will be utilized by the Cyber-Range sub- model to drive the different phases of the training scenario. For the purposes of the training also different threat actors will be considered.

3.1.2 Cyber-Range training

A cyber range training is defined as a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organization's ICT, OT, mobile and physical systems, applications and infrastructures [7] It , includes the simulation of attacks, of users and of their activities and of any other Internet, public or third-party services which the simulated environment may depend upon.[7]. An exhaustive survey on Cyber range architectures in relation to training may be found.[13]
The Cyber range training program sets one or more expected trace to track the progress of a user during its training. For example, if an end-user examines a malicious email that contains a link, the expected trace is to monitor if the user presses the link or not. In this example, but if the scenario involves a security expert that needs to investigate the origins of the link, then the training program will check the users investigation path identified by the trainee.
The training program sets one or more expected trace to track the progress of a user during its training. [6]
The cyber range will provides a place to practice correct and timely responses to cyber-attacks and the participants can practice skills such as network defense, attack detection and mitigation, penetration testing, and many others in a realistic environment
The Cyber range training program will allow one more training program executions each characterized by a set of permissible actions. (the typical end users has a set of permissible actions different from the one of a security expert).

The implementation of the Cyber Range training will be accomplished through emulation and simulation of the components and the interactions among them. A training program may involve more than one simulation and emulation sub-models.
Implemented sub-model will accommodate a detailed representation of marine simulation environments and its components in order to support automatic generation of the simulation demands of the training program. [6] and [12]
It will be explored the actual feasibility of an automatic cyber range instantiation for real effective cybersecurity training. In fact reutilization of cyber ranges environments for any subsequent training sessions, even if acceptable someway, bounds the quality of the training, since the environments cannot be quickly updated if the need arises and is a possible cause of possible information leakage decreasing the effectiveness of the cyber range as a skill-evaluation tool.
Furthermore, the proposed model-driven approach to Cyber-Range training is based on the definition of a Security Assurance Model that enables the systematic representation of the target organization, its assets and their relations, and, ultimately, its security posture.[6].

3.2 **Training program**

Training will be descripted in accordance with infrastructure and ship information technology (IT) and operation technology (OT) as described in [4]. The training environments used in cybersecurity training are typically known as cyber ranges [5]
We will identify the most critical security aspects for each organization and will customize a training program. The training perspectives will be recorded in the training sub-model. This includes the learning objectives for each trainee type and the organization as a whole, as well as the dynamic adaptation and skill development features [12]
During the initial analysis phase it will be analyzed the environment using for example the guideline of STRIDE methodology designed by Microsoft. It includes the following threat categories: (i) Spoofing, (ii) Tampering, (iii) Repudiation, (iv) Information disclosure, (v) Denial of Service (DoS), and (vi) Elevation of privilege.[4].
Trainees can reach competence in cyber-security mainly via hands-on learning with virtual labs led by an instructor. Therefore, a proper training program must incorporate a series of good content and tutor interaction, pedagogical framework, and essential virtualized exercises for hands-on interplay.
It is widely accepted that an exercise should be defined in three phases [4], namely:

- planning the scope and objectives,
- implementation, and
- evaluation/feedback.

The training program that will be proposed will use hands-on activities for developing practical abilities, so as to ensure that trainees can subsequently deal with real-life incidents [5]. Once the trainee has completed the basic training for a learning unit, further models are activated and the trainee can now proceed with the advanced training.
Initially it will be established a training program tailored to organization specific a complete learning path needs and then it be modelled
Customized training scenarios will be developed under Cyber Range to support trainees to effectively and systematically utilize different security tools learning the procedure for various types of actions e.g. preparedness, detection and analysis, incident response, post incident response) and security processes in their work organizations (according to different types of users of the system (e.g., end-user, administrator, technician, security engineer, blue/red team).
Training content will be customizable for the target audience (as large as possible) on the basis of knowledge and ability levels, in particular :
Implemented training content will be created in accordance with the skills that the program aims to develop;

- The training program will make use of hands-on activities for developing practical abilities, so that that trainees will be able to deal with actual cases.
- The training program will be sustainable on long term.

These requirements will be translated into two important features :

- Ability to modify and add new training content in an easy manner;
- Ability to create and manage the training environment.

The Training Program will be designed to include or feature:

- A brief description

- A measurable goal for the training (just for example in a phishing scenario, the trainee might have to identify at least 80 percent of the phishing emails);
- Roles that the program is programmed to train (e.g., end-user, administrator, technician, security engineer);
- Types of training (e.g., analysis, detection, preparedness, security awareness);
- A difficulty value that indicates the difficulty rating (e.g. a phishing training scenario might be from simply to considerably complex).
- Covered assets, (tangible and intangible for example damage to an equipment or breach into data)
- Threats, security controls

After the completion of the training, the platform displays the results for each trainee and the program as a whole will be displayed. This process will show indicates the scores of the trained personnel and their achievements regarding the educational processes.
After the completion of the training, the Cyber range platform will displays the results for each trainee and the program as a whole. This process indicates the scores of the trained personnel and their achievements regarding the educational processes.
As per [4] basic training will be considered successful when the trainee:

- Has mastered the main teaching material;
- Has passed the training evaluation (e.g., exercises, exams, etc.) with an adequate score;
- Has passed a game, which contains all the involved learning topics of the learning unit, with an adequate score.

Once a good level of understanding has been accomplished by the trainee, he/she can proceed with the related advance training scenarios.

3.2.1 User interface

The user interface (UI) will be intended for the training organizers. The UI will make it possible for organizers to decide the content of a particular training session as easily as possible. The UI will be based on a wizard-like approach and will guides the organizer through selecting the type of training for example.
The user interface will employ a wizard-like to help the organizer through selecting the type of training the object of training and the training difficulty level [5]

3.2.2 Programmed development

The overall cyber range package will generate the training content for a particular training session based on training organizer input and possibly upload it to an e-Learning system and simultaneously, will create the cyber range training environment corresponding to that training content .
Simulation Sub-Model
The Simulation Sub-Model is responsible for indicating if a component can be simulated and is describing the simulation environment and its individual components [12]. The simulation model specifies for example

- the asset
- the deployment mode for the simulated component
- tool is used to implement the simulation
- the required, initialization operations
- the time and date that the simulation started and ended;
- the current simulation and date time;
- the execution speed
- the random seed value that influences the random operations of the simulation in order to have reproducible randomness; the list of messages that are exchanged among the simulations modules (e.g., events, commands,
- different scenarios are envisaged targeted to users with different responsibilities and level of expertise.

3.2.3 Functionality Evaluation

There will be performed three classes of technical assessment techniques [5] [7]:

- Review techniques: Documentation review, log review, ruleset review, system configuration review, network sniffing, and file integrity checking;
- Target identification and analysis techniques: Network discovery, network port and service identification, vulnerability scanning, and wireless scanning;

• Target vulnerability validation techniques: Password cracking, penetration testing, and social engineering.

4. CYBER-MAR TRAINING AND AWARENESS RAISING

Cyber-MAR (Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain), a 3 year project that began in September 2019, funded through Horizon 2020, has the following objectives : “it is an effort to fully unlock the value of using cyber range in the maritime logistics value chain via the development of an innovative simulation environment adapting in the peculiarities of the maritime sector, and being at the same time easily applicable in other transport subsectors”.

It aims to cover the training needs for all professionals (cyber-security/IT experts ,non IT-expert personnel of ports, shipping operators, linked entities influenced by possible cascading effects) and most importantly raise the cyber-threat awareness level within those organisations thanks to hands-on training.

Cyber-MAR is implementing a new educational hybrid approach, offering practical, operational and hands-on training, that will be developed as Physical training sessions, Virtual training sessions through Cyber-MAR LMS, Simulation activities through Cyber- MAR CR, pilot activities (2 in ports and 1 in shipping environment.

The Cyber-MAR LMS one of the core components of Cyber-MAR platform (CyberMAR Cyber Range, Cyber-MAR LMS, CyberMAR MaCRA, Cyber-MAR econometric models) will be addressed to all involved actors aiming at raising awareness at all levels within an organization, providing practical training.

The hands-on training that will be offered as par of the project will develop on situational images of the IT state of the target system of the different actors involved who will participate in the training. Thanks to the development of visualization tools, during the exercises, the aim is to provide an image of situational awareness almost in real time of the attacks / defenses and about the state of the system. Trainees can view low or high-level information relating to the event that occurs (attacks, defenses or systems status) with the related temporal information. In order to show the trainees what may have been tampered with in the system, the forensic evidence could be attached to the situational picture. It is very important for trainees to have a clear timeline of the scenario, with the necessary contextual information: this will allow them to provide feedback and request support for the specific scenario after execution.

From an initial analysis carried out, the training levels (table 1) and target groups identified for the purpose of participation were defined (Table 2).

The users involved vary from simple users who do not have basic knowledge on the current threat landscape and how to use the related defense mechanisms, to security experts, who have high IT security skills, as well as practical experience in responding to security incidents. Users who will be able to access the intermediate level are more familiar with Cyber-security. Cyber-MAR trainings will be developed on three levels:

- Entry level: aimed at users who have no basic knowledge of cyber-security. Aspects of the problem will be dealt with on a theoretical level in order to familiarize the public with the concept of IT security and to raise awareness among identified users. The course will cover the basic introduction to cyber security to the concept of Cyber-MAR. Attendees will have the opportunity to understand cyber security threats and basic concepts for reducing risk in the maritime sector.
- Mid - level: aimed at users with greater familiarity with the topic. The course aims to provide an overview of the risks for cyber security in the maritime environment, introducing the Cyber-MAR concept and its platform.
- Advanced level: aimed at an audience of experienced users in IT security. The course will provide a more detailed overview of cybersecurity risks, as well as help determine how effective risk assessments will be in reducing threats and vulnerabilities in the maritime sector (with cascading effects) by leveraging the Cyber-MAR approach.

Table 1. Training levels

Complexity level	Details	Requirements	General aims
Entry level	Entry-level users who are not familiar with cyber security **Theoretical**	Basic skills about TCP/Ip and/or network security in reality, nothing officially required since the training will take them into that space for the first time and will be used to grant access to the second level	Training is a basic introduction to cyber security and the concept of Cyber-MAR. The goal is to raise awareness among identified users (very large audience). To give the participant the opportunity to understand cyber security threats and the basic concepts for reducing risk in the maritime sector.
Mid level	Users who are familiar with cyber security and wish to increase their skills to a higher level **Theoretical and hands on**	Middle level : it's a must that they have at least 3 years of experience into networking and security and to have got entry level certificate	The course aims to provide an overview of cybersecurity risks in maritime domain, introducing the **Cyber-MAR concept** and platform (familiarisation)
Advanced	Users with high IT security skills, at theoretical and practical level. High security specialists may work as senior positions in IT departments. **Theoretical and hands on**	Mid level certification plus direct experience on specific security environment , nice to have certiffications on cybersecurity and vertical skills like CEH, Comptia Security +, CCDA and ISACA CISM and/or CRISC, but nice to have, not a must have	The course aims to provide a more detailed overview of cybersecurity risks and how good risk assessment will have a positive impact in reducing threats and vulnerabilities in the maritime sector also through the Cyber-MAR approach. The course will be updated with the latest tools on the use of the Cyber-MAR CR together with the recent international legislation and guidelines. Deep dive in cyberMAR and CR platform

Source: own elaboration

Table 2. Target groups

Primary Levels of attendees	Details	Specific groups/level
Management	People responsible for parts of the infrastructure and/or services it provides. They've an overview of the business processes whitin organization, however they don't have technical expertise.	1. Maritime Professionals and administrative staff (port authorities, operators, associations, freight transport & logistics actors) 2. Port authorities, operators and associations 3. Governance/Regulatory organisations, public authorities, Classification Societies 4. Admins/operators (Systems management, system administrators, network engineers)
Users	End-user who uses the infrastructure to as a means to conduct their work.	1. Academia (Universities, Research Centers & Institutes, Laboratories, Student Communities) 2. Engineering/Consultancy 3. Users and special communities
		4. CERT/CSIRTs network
Technical people	Staff at different levels of organizations/infrastructure.	1. Security specialists 2. ICT Companies 3. Engineering/Consultancy 4. Cybersecurity SMEs

Source: own elaboration

5. RESULTS

The first LMS - Entry-level for training was held in November 2020 and the participants belong to different target groups, as shown in Figure 1.

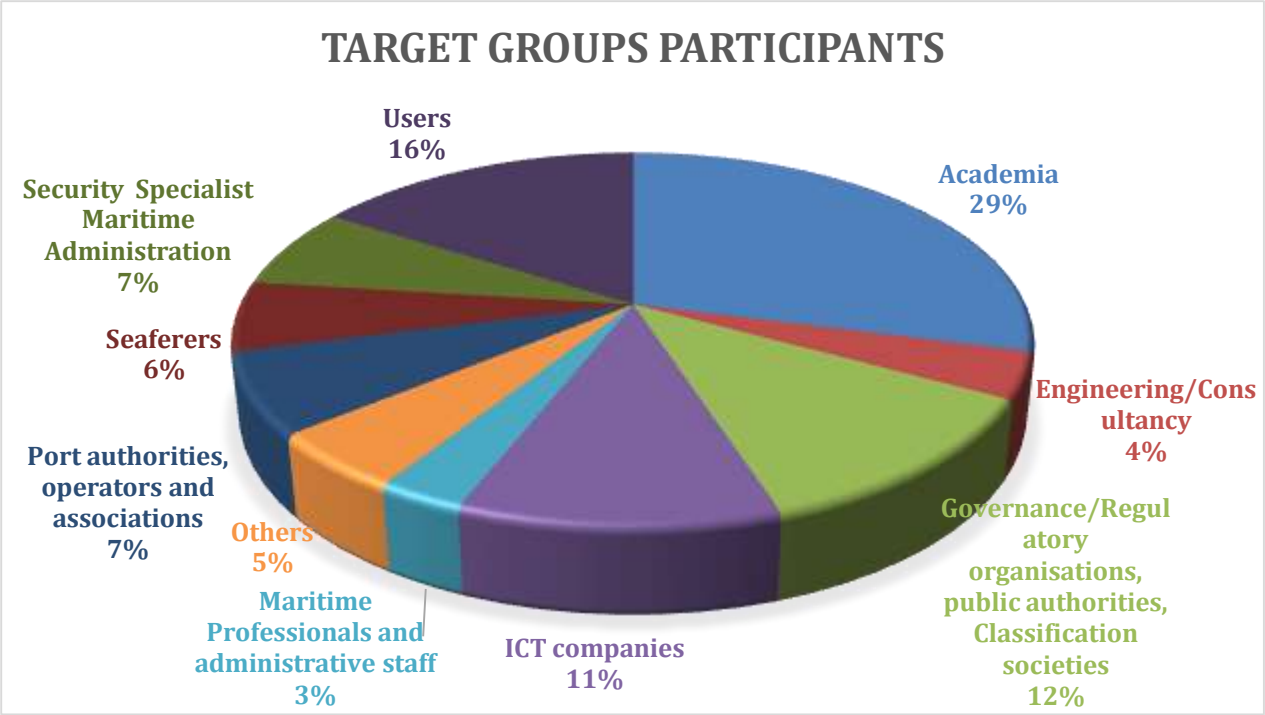

Figure 1. Target groups (source: own elaboration)

The "maritime officer" and "maritime management" account for almost half of the participants, followed by the "Academia" group (university, research and education). The “Others” (5%), include consultants and journalists. About 11% from ICT companies ", and 6%" maritime ".
The interest from the maritime community (maritime administrations, seafarers) shows that there is an awareness of acquiring more knowledge on maritime cyber security issues. Moreover, from post-training surveys filled in from the participants issued the necessity to create a maritime cyber-security culture.
Furthermore, from the surveys, it emerged that 58% of the participants fully agree that the training has gained more knowledge applicable to their work, 30% agree while the remaining 12% are neutral.
Among the topics addressed, the most appreciated were the case studies of maritime cyber attack and how to countermeasure in the organizations.

6. CONCLUSIONS

The maritime sector is under an ongoing digitalization process in all operational aspects. Lack of knowledge of security procedures and awareness is a common issue that is further exacerbated by the rapidly changing technological scenarios.
Training and awareness should be tailored to the appropriate levels for different figures in the maritime community, both on board and ashore.
To respond to the growing need to increase safety levels, it would be necessary to create an awareness or training framework for personnel working in the maritime sector.
And this is demonstrated by the first results of the Cyber-MAR training that demonstrate the willingness on the part of the participants to increase knowledge and awareness on security, in a sector that is experiencing a process of digitization in all operational aspects. , which is further exacerbated by the rapid technological scenarios.

“Cyber-MAR project has received funding from the European Union’s Horizon 2020 research & innovation programme under grant agreement No. 833389. Content reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains”.

REFERENCES

[1] [1] Dalaklis, D. and Schröder-Hinrichs, J.U. “The Cyber-Security Element of Hybrid Warfare: Is there a Need to “Formalise”, Training Requirements?” 10th NMIOTC Annual Conference (“Countering Hybrid Threats: An Emerging Maritime Security Challenge”), Chania-Greece, 4 June 2019

[2] [2] Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D., “A novel cyber-risk assessment method for ship systems. Safety Science”, 131, 2020

[3] [3] Cyber-MAR project, Accessed 03 January, 2021, https://www.cyber-mar.eu/

[4] [4] G. Hatzivasilis, S. Ioannidis, M. Smyrlis, G. Spanoudakis, F. Frati, L. Goeke, T. Hildebrandt, G. Tsakirakis, F. Oikonomou, G. Leftheriotis, and H. Koshutanski, “Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees,” Applied Sciences, vol. 10, no. 16, p. 5702, Aug. 2020

[5] [5] Beuran, R.; Pham, C.; Tang, D.; Chinen, K.; Tan, Y. and Shinoda, Y. “CyTrONE: An Integrated Cybersecurity Training Framework.” In Proceedings of the 3rd International Conference on Information Systems Security and Privacy - Volume 1: ICISSP, 2017

[6] [6] Somarakis, Iason, Michail Smyrlis, Konstantinos Fysarakis and G. Spanoudakis. “Model-Driven Cyber Range Training: A Cyber Security Assurance Perspective.”, 2019

[7] [7] European Cyber Security Organisation (ECSO), "Understanding Cyber Ranges from Hype to Reality" (White Paper) rel. 30-March 2020

[8] [8] K. Tam, K. Moara-Nkwe, and K. D. Jones, “The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training”, Marit. Technol. Res., vol. 3, no. 1, pp. 16-30, Jul. 2020

[9] [9] Hautamäki, J.; Karjalainen, M.; Hämäläinen, T.; Häkkinen, P. “Cyber security exercise: Literature review to pedagogical methodology”. 13th annual International Technology. In Proceedings of the Education and Development Conference, Valencia, Spain, 11–13 March 2019

[10] [10] McDaniel, L.; Talvi, E.; Hay, B. “Capture the Flag as Cyber Security Introduction”. In Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016

[11] [11] James, J.E.; Morsey, C.; Phillips, J. “Cybersecurity education: A holistic approach to teaching security. In Issues in Information Systems”; Maria, E.C., Ed.; IACIS: Leesburg, VA, USA; Volume 17, pp. 150–161, 2016

[12] [12] Yamin, M. M., Katt, B., & Gkioulos, V., “Cyber ranges and security testbeds: Scenarios, functions, tools and architecture”. Computers & Security, 88, . 2020

[13] [13] Cyberwiser.eu, Accessed 03 January 2021, https://www.cyberwiser.eu/content/what-cyber-range

[14] [14] Cyberwiser.eu, Accessed 02 January 2021, https://www.cyberwiser.eu/smes-cybersecurity-best-practices-assessment

[15] [15] 1st Global Cybersecurity Observatory, Accessed 02 January 2021 https://cyberstartupobservatory.com/cyber-range-what-it-is-what-it-is-not-and-what-it-will-be/

[16] [16] Cloudshare, Accessed 03 January 2021, https://www.cloudshare.com/virtual-it-labs-glossary/what-is-a-cyber-range

[17] [17] Steve Morgan, 2019 Official Annual Cybercrime Report Retrieved from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf)

[18] [18] Annie Reiss, Don’t Let Poor IT Training Freeze Your Productivity, 11 February 2019. Retrieved from https://www.cloudshare.com/blog/dont-let-poor-training-freeze-productivity

[19] [19] Hackernoon, Accessed 03 January 2021, https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700

[20] [20] Kish, D.; Carpenter, P. Forecast Snapshot: Security Awareness Computer-Based Training, Worldwide. 2017. Gartner Research, ID G00324277, March 2017. Retrived from https://www.gartner.com/en/documents/ 3629840/forecast-snapshot-security-awareness-computer-based-trai