M. Canepa
World Maritime University
moc@wmu.se

R. Hopcraft
University of Plymouth
rory.hopcraft@plymouth.ac.uk

S Karamperidis
University of Plymouth
stavros.karamperidis@plymouth.ac.uk

F. Ballini
World Maritime University
fb@wmu.se

Cyber-MAR dynamic Awareness Raising – An Integrated Maritime Cyber Risk Management Approach

Abstract

The ISM code, supported by IMO Resolution MSC.428 (98), requires shipowners and managers to ensure that cyber risks are adequately taken into account in safety management to implement relevant measures in all functions of their safety management system, up to the first Document of Conformity after 1 January 2021.

The entry into force of the new IMO regulation requires ships to integrate IT risk assessment into their safety management systems.

The above represents a turning point in IT security onboard ships, introducing the concept of cyber risk management in the maritime sector.

In this phase of application of the legislation, it is helpful to adapt correctly by learning from the important cyber-attacks that have targeted the navigation and shipping sector by the sea in recent years. Therefore, cyber risk management currently represents a significant challenge for the maritime sector, and training is one of the key factors in winning the challenge.

This paper will explore how, through the implementation of dynamic training

approaches related to the Cyber-MAR project, cyber awareness is increased. It can constitute a valuable tool for responding to a company's cyber risk management.

Keywords: *Cyber dynamic awareness raising, maritime cyber risk management, hybrid training, maritime transport, digitalization*

Acknowledgements

The authors acknowledge financial support from the European Union's.

"Cyber-MAR project has received funding from the European Union's Horizon 2020 research and 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".

1. Introduction and Background

In the last decade, there has been a progressive and significant transition from an analog to digital approach in the maritime sector. This transition was driven by three main elements:

1) need for operational costs reduction
2) increase visibility in the supply chain
3)Path to digitalization

Cyber-attacks are growing in number and sophistication. To safeguard maritime operations, data and assets it is necessary to minimize vulnerabilities and to use extensively and efficiently tools to recognize attacks and implement countermeasures.

Awareness is the state of being conscious of something. More specifically, it is the ability to directly know and perceive, to feel, or to be cognizant of events. Indeed Humans are the most important factor in cyber resilience, they must be receptive in understand risk associated to their operations.

Personnel training provides cyber-security professionals with the knowledge and capabilities required to confront cyber-attacks. Personnel awareness refers to knowledge of the characteristics, contents, and criticalities of IT security within organizational structures.

The goal of the Cyber-MAR project is to establish a cyber ecosystem for simulating a cyber-attack, and estimating the impact of cyber-attack from a technical and financial point of view.

From a conceptual point of view the Cyber-MAR project has been developed to create a specific cyber range environment and use it at three levels:

- People: training sessions and involvement in the pilot actions
- Procedures: covering the identified gaps,
- Technologies: procedure testing as support to identify complex vulnerabilities

The purpose of the ISM Code is to provide this standard. It is supported by IMO Resolution MSC.428(98), which requires shipowners and managers to ensure that cyber risks are adequately taken into account in safety management to implement relevant measures in all functions of their safety management system, up to the first Document of Conformity after January 1 2021.

1.1 General facts

At the end of 2020, the European Union's Horizon 2020 Cyber-MAR project demonstrated the implications of a cyber-incident targeting European maritime infrastructure. It has been put into evidence that through the opening of a malicious email, malware is able to spread throughout a port's digital infrastructure. Eventually the malware propagates through all parts of the ports IT systems allowing an attacker to control the power management system.

1.2 Cyber threats and tools

Cyber threats targeting systems' vulnerabilities have being existing since a long time; they are increasing in sophistication and potential danger more and more. Cybersecurity education and training are becoming increasingly relevant as the only way to prevent and handle such cyber breaches adequately. This paper elaborates analysis of training education and assessment its basis is in part derived from CyTrONE (Cybersecurity Training and Operation Network Environment) (Beuran, 2018).

Training is approached as Dynamic training that is a living, breathing tool that is constantly updated, contextual to day-to-day needs, engages users with critical thinking and actually empowers them to learn skills and fix problems (Urias,2017).

2 The human element in cyber safety management

The maritime sector has always relied upon human involvement from sailing the ships to operating the port cranes (Kia et al., 2000). While these roles have changed or been replaced with the integration of technology, maritime operations are still significantly reliant upon human operators [ibid]. Figure 1 illustrates the major fields on employment in the maritime sector. Many of these roles are directly involved in the safety of maritime operations.

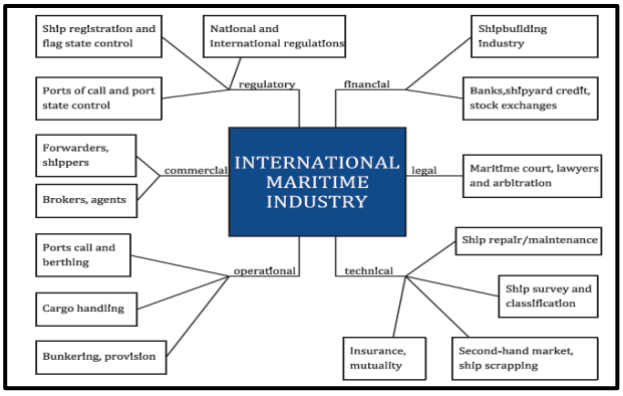

Figure 1 Major fields of employment in the maritime industry (International Organization for Standardization, 2020)

What is evident from the variety of employment fields in the maritime sector is that each personnel has a different role to play in safety.

The last and final barrier normally involves the operator of the system. The human element is sometimes referred to as the biggest internal threat facing the cybersecurity of companies (Boletsis et al., 2021, Meshkat et al., 2020).

Following the argument that humans are often the last barrier to stop an incident occurring, Singleton (1973) argues that the cause of almost any incident can be traced back to inadequate design, inadequate training, inadequate instruction or inadequate attention resulting in a human error. Barnett (2005) illustrates the different types of human error (see Figure 2).

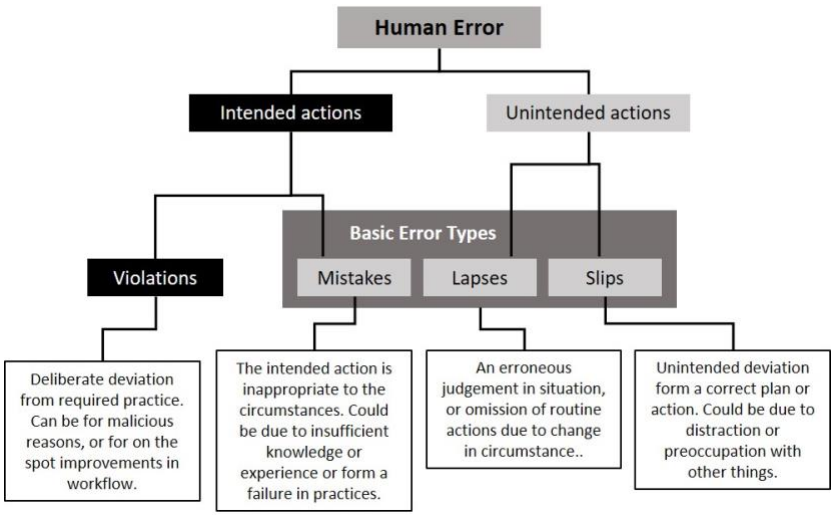

Figure 2 Summarised Sources of Human Error (adapted from Barnett 2005)

Therefore, regardless of the various layers of safety that have been built into a system, human error, accidental or deliberate can allow an incident to occur. the

safety training provided needs to be appropriate to people specific roles.
As a part of the ISM Code companies are required to develop and implement a safety management system (SMS) to be complied with by personnel.

3 Cost Vs effectiveness

Cost-benefit analysis is a method used to evaluate a project by comparing its losses and gains. Generally the investment is evaluated using the Gordon Loeb Model (Willemson,2010) . The Gordon–Loeb model is a mathematical economic model used to analyze the optimal investment level in information security.
Investing to protect company data involves a cost that, unlike other investments, usually does not generate profit. It does, however, serve to prevent additional costs. Thus, it's important to compare how expensive it is to protect a specific data set with the potential loss in the case data is stolen, lost, damaged, or corrupted.

3.1 Evaluation of investment

Given the importance of cybersecurity to the survival of an organization, a fundamental economics-based question is:

"How much should be invested in cybersecurity-related activities?"

Since organizations have finite resources, answering the above question involves a resource allocation decision. A good starting place is to assess the costs and benefits (i.e., conduct a cost-benefit analysis) associated with cybersecurity investments. The optimal level of cybersecurity investment for an organization is the point where the expected marginal investment costs equal the expected marginal benefits derived from the investment.

It is important to compare how expensive it is to protect a specific data set with the potential loss in the case said data is stolen, lost, damaged or corrupted.
The amount of money a company spends in protecting information is, in most cases, only a small fraction of the predicted loss (for example, the expected value of a loss following a security breach).

3.2 Return On Investment (ROI)

At a basic level, one way of calculating cybersecurity ROI involves taking the average cost of an incident and multiplying that number by how many incidents a business might experience in a given time frame.

Return on investment (ROI) is a "metric" used to understand the profitability of an investment. ROI compares how much it has been paid for an investment

to what it has been earned so that it is possible to evaluate its efficiency.
ROI in cyber security or Return on Security Investment (Losi, 2006), (ENISA, Introduction to Return on Security Investment no date) allows companies to measure the KPIs (Key Performance Indicators) of projects .

3.3 How to calculate the ROI of investments in cyber security

The ROI of investments in cyber security is not calculated in the same way as the ROI for common investments is usually determined. Some examples are given below.

3.3.1 The BCG Platinion method

The first method for calculating ROI was developed by an American company, Boston Consulting Group (BCG). In particular, from the BCG Platinion a branch of Boston Consulting, that deals specifically with IT and cyber security. According to Michael Coden, director of the cyber security department of BCG Platinion, to calculate the ROI on an investment in cyber security, the following formula is used:

Cybersecurity ROI = [(Expected losses before the project) - (Expected losses after the project) - (Project cost)] / Project cost

Expected losses are calculated by multiplying the impact of a possible event by the probability that this event will happen.
With the BCG Platinion method the ROI is positive if the cost of the cyber security project is less than the difference in the expected losses before and after the project itself.

3.3.2 The method of the SANS Institute

Another widely used method is the one developed by the SANS Institute
The formula for calculating the ROSI (Return on Security Investment) is:

*ROSI (%) = (ALE * Mitigation Ratio - Cost of solution) / Cost of Solution*

Where ALE is equivalent to the "Expected losses before the project" of the BCG Platinion model.

The Mitigation Ratio, on the other hand, is a percentage that indicates how much the probability of an adverse event would be reduced if the cyber security project were financed. This model provides a percentage of damage reduction. In this model, to have a positive ROI it is necessary not only that the ALE is higher than the cost of the cybersecurity project, but also that the Mitigation Ratio reaches a

percentage such that the expected post-project losses are lower than the cost of the project itself.

3.4 Conclusion about cost-effectiveness

Regardless of the formula used, it is essential for decision makers to have effective tools at their disposal to be able to assess in detail the extent of the positive effects of an investment in cyber security.

4 Basics of the approach Ciber Risk Management

People must be have the appropriate skills and experience to ensure that the human element is able to provide a valuable addition to cyber risk management practices. The only way to have these skills is through appropriate training.

Even a small investment in security awareness and training has a good chance of significantly reducing the business impact of a cyber-attack.

4.1 Initial considerations on weakness

1) Attacks are on the rise as more employees are working from home
2) Humans are a considered a weakness in an organizations cybersecurity
3) Compliance requirements for businesses and operations are increasingly focused on employee training
4) Providing basic training is not enough to educate employees - Creating regular training is the best way to provide employees with the knowledge to effectively respond to cyber threats.

4.2 Risk based approach

A risk-based approach to cyber security enables an organizations to identify which of their assets or operations represents the highest risk and allocate resources accordingly. Priority of actions should be evaluated regularly as various factors change, including criticality of the system, value of the asset, new known attacks or vulnerabilities etc. After the asset priority list has been created, it is necessary to assess the vulnerabilities of each so that risk is included and analyzed in the organizations business risk management.

4.3 Training vs Awareness - A cost-effective approach to cyber security

In the NIST Special Publication 800-16 (Wilson 2003), security awareness has been defined as followed: "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security".

Cybersecurity awareness involves being mindful of cybersecurity in day-to-day situations. Being aware of the dangers of browsing the web, checking email and interacting online are all components of cybersecurity awareness.

5 Development of training

When developing training it is important to consider the level of responsibility each personnel has for risk management. As illustrated in Table 1each level requires more knowledge but helps to ensure a better understanding of the risks that digital technology poses.

Table 1: Description of Cyber-MAR Training Levels (Authors own elaboration)

Complexity level	Details	Requirements	General aims
Entry level	Entry-level users who are not familiar with cyber security **Theoretical**	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 (familiarization)
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 certifications 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 Cyber-MAR and CR platform

The Cyber-MAR LMS provides an accessible training environment that will complement existing qualification pathways offered by public and private entities. Moreover, it will provide a dedicated training cyberspace and a maritime logistics simulation environment for an integrated training and simulation environment.

From an initial analysis carried out, the training levels (**Error! Reference source not found.**) and target groups identified for the purpose of participation were defined (**Error! Reference source not found.**).

6 Cybersecurity Effectiveness

Cybersecurity effectiveness can be evaluated by how much time lapses between the detection of a threat and when appropriate actions are taken.

6.1 Which metrics

Establishing some key metrics to determine cybersecurity effectiveness is an important point, any organization should start by putting into relation their business goals with how enhanced security can help to achieve those specific goals. Some examples of various metrics are shown below.

- Current Capabilities Status: it is the list current security capabilities, for example what programs are in used?
- List of vulnerable assets: knowledge about the number of all vulnerable assets.

6.2 Test metric effectiveness

Effectiveness is generally assessed in terms of:

- Track patches and updates - Patch management is a critical aspect of addressing vulnerabilities in software.
- Response Time - Tracking response times for a variety of incidents is a relatively objective and efficient way to measure overall effectiveness.
- Monitor data transfer: Monitoring the volume of data being transferred will help an organization identify misuse.

6.3 What steps can a company take to fill performance gaps?

Companies can:

- Continuous education Educate Employees
- Systems update
- Detection and recovery time.

After completing the above steps, an organization has a better understanding of the effectiveness of their cybersecurity program and how it aligns with their overall business goals.

7 Cyber Range based 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.
The training program will incorporate a series of dedicated content, interaction, the pedagogical framework, and important virtualized exercises for hands-on interplay.

7.1 Cyber-Range training

A cyber range training (Canepa 2021) 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.

The Cyber range training program allows one more training program execution, each characterized by a set of permissible actions. (The typical end users have a set of permissible actions different from a security expert).

7.2 Training Program

People are generally considered the weakest link in a computer system, so that a professional training is 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.

Training requires proper framework that needs to be easily and quickly configured. The key is automating the training content generation and environment setup tasks, modeling the scenarios accurately. Training groups by Cyber-MAR (Table 2) are targeted to:

- Management
- Users
- Technical people including the ones that support operations of the ship

Table 2 Description of Cyber-MAR Target groups (Authors own elaboration

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 within 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-users 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

As the trainee accomplishes their basic evaluation tasks, the training program starts involving more advanced features that demand a higher level of understanding. Three phases with increasing difficulty is proposed. The overall method is integrated in a cyber-ranges platform.

From an initial analysis, the training levels (Table 1) and target groups identified for participation are defined (Table 2).

The users involved vary from simple users to skilled ones:

- Entry level: aimed at users who have no basic knowledge of cyber-security
- Mid - level: aimed at users with greater familiarity with the topic
- Advanced level: aimed at an audience of experienced users in IT security.

7.3 Development of the training program

Many studies (Canepa 2021), show that the use of multiple training methods may provide the highest consciousness about perceived security effectiveness in employees. These different methods can include both face-to-face training or e-learning and they could also have practical sessions allowing a hands-on approach to training.

7.4 Learning management system

To help improve the cost-effectiveness of the development and delivery of cyber security training it is important to consider the development of a learning management system (LMS). For example, the Cyber-MAR LMS will provide an easily accessible training environment that will complement existing qualification pathways offered by public and private entities. Moreover, it will provide dedicated training in cyberspace and a maritime logistics simulation environment

for an integrated training and simulation environment. Keeping training in a central management system ensures all staff is able to access the materials and training they require in a timely and cost-effective fashion. Moreover, the LMS allows a company to monitor its personnel's training, ensuring they complete content as required. This in turn, ensures that personnel remains up-to-date with the latest developments in risk management practices, helping to reduce the risks of a cyber incident.

Finally, as above has mentioned, determining the content of this training is a vitally important step. Developing a comprehensive syllabus ensures that training is representative and appropriate to a company's risk profile. Ensuring the syllabus considers a company's everyday operations, systems, and personnel skillsets. As such, the primary aim of the training is to ensure that personnel can respond appropriately to a cyber incident to ensure the ship's and crew's continued safety. This personnel also need to be able to respond to these incidents, and know how to communicate important details of the incident to management or specialized companies.

Looking to the nuclear industry where safety training is critically important there is some guidance that can be applied. The content of these courses ensure companies are thinking about their risks, and subsequently associated risks, before developing training content. This understanding is then built into the training, ensuring that personnel understand the mitigation measures and the cause of the risks. It allows them to make holistic decisions about risk, as they are better prepared to spot when situation is starting to become unsafe. Developing content in this way ensures that the right knowledge about the high-priority risks is passed on to personnel. This ensures that the development and suitability of the training remain cost-effective, where it will have the largest cost-to-benefit improvements.

The Cyber-MAR project adopted a approach used in nuclear industr to its training development and assessment (Dalaklis 2019), and the results are positive from recent feedback and surveys on delivered training. For instance, the overall satisfaction score for the training session was 4.6/5.0. The variance in scores was very low (standard deviation of 0.1746) indicating consistent responses.

8 Content of the courses

Course contents is outlined in the tables that follows:

Table 3 - Course Entry level

Cyber-MAR Training

Entry Level					
Overall Learning Outcome	Introduce core themes and terminology to raise awareness of cyber security threats to the maritime sector and prepare the audience to the Intermediate level participation.				
Training Methods	Webinars, MOODLE				
Comments	Splitting the Entry Level in this way provides both an overview of cybersecurity for all members of the maritime sector, while allow some differentiation for managers who may need to know a little bit more to make informed decisions about risk assessment and management. This is also a good place to introduce the three pilot scenarios as discussion points on how these attacks occur as well as appropriate risk management practices.				
Topic	**Target Group**	**Learning Outcomes**	**Hands on Activities**	**N. Hours**	**Prerequisite Knowledge**
Cybersecurity Awareness	Users Management E & R	Introduce core cybersecurity themes and discuss their relevance to the maritime sector	Webinars Quiz	9	Basic IT skills, use of standard systems like emails, web browsers, computers in general
Managing Cybersecurity	Management Technical E & R	Discuss why the effective management of cyber-attacks is important for a business, and provide some methods for managing that risk.	MOODLE	2-3	Knowledge about maritime real-life procedures and business needing --

Table 4 - Course Mid level

Intermediate Level					
Overall Learning Outcome	Introduce users to the Cyber Range, and provide a basic level of awareness of how the system operates, and information that can be gained from it. Basic view about OT security.				
Training Methods	MOODLE, Face-to-Face workshops				
Comments	These modules are designed to walk the user through their first-steps of using the platform. It is less important that managers are provided with in-depth training as they are likely to pass this off to the IT departments. The reason for the manager specific module is to provide a single session that provides them with enough information to use the platform to run the configurations that the IT department have designed, to allow them to inform their risk management decisions. This addresses Naval Groups concerns about including econometric models etc. The three pilot scenarios can be used to demonstrate how the platform works and the information that can be gained from them. IT and OT will need to start joined activities				
Topic	**Target Group**	**Learning Outcomes**	**Hands on Activities**	**N. Hours**	**Prerequisite Knowledge**
Introduction to the Cyber Range	Management Technical Users E & R	Provide learners with the support to install and access the cyber range. Walk users through the user-interface exploring the key features of the platform	MOODLE Workshops	2-3	Basic use of computers and systems --
Basic Tools for a Cyber Range	Technical E & R	Provide users with the knowledge of how to See and Search, users, objects and topologies *(VIEW ONLY)* Basic knowledge of data mining techniques to explain how the platform works.	Workshops MOODLE	4	TCP/IP networking protocol, routing, switching fundamentals
Using a Cyber Range to Understand risk	Management Technical Users E & R	Provide a high-level overview of the Cyber Range and how to run the product of the IT Departments configurations. Explore the information that can be gained from this and discuss how this can be useful in managing cyber risk (Econometric models and Remediation Plans).	Workshops MOODLE	4	--
Lesson learned from Cyber MAR pilots: Cyber-attack scenario on the Valencia port authority's electrical grid	Management Technical Users E & R	Real life activities will provide to users a better understanding of risks targets attacks damages and remediation	Workshops MOODLE	1	--

Table 5 - Course Advanced level

Advanced Level					
Overall Learning Outcome	Provide users with the required skills to be able to manipulate the cyber range, and create realistic scenarios that allow them to provide much needed information to decision-makers. Intermediate view about OT security.				
Training Methods	MOODLE, Face-to-Face				
Comments	At this level users are given the skills to use and change the cyber range to suit their needs and requirements. This level also provides a module that explores how companies can use the platform to develop scenarios that are relevant to them, and how these can be used to help inform risk management practices. Walkthrough of how to create the various pilot scenarios, as a demonstration of how to manipulate the platform. IT and OT will learn mutual correlations.				
Topic	**Target Group**	**Learning Outcomes**	**Hands on Activities**	**N. Hours**	
HNS Pro user training	Technical E&R	Provide users with the ability to make changes within the platform, including managing and creating objects, topologies and scenarios.	Workshops MOODLE	4	TCP/IP networking protocol, routing, switching fundamentals. Network security – design. Advanced system management (prevention)
Crafting an Attack (Theory)	Management Technical Users E&R	Provide learners with the understanding of how to develop and design their own cyber scenarios that are considerate of the platforms limitations.	Workshops MOODLE	2-3	TCP/IP networking protocol, routing, switching fundamentals. Network security – design. Advanced system management (prevention)
Crafting an Attack (Practical)	Technical E&R	Utilising the knowledge gained in the previous training, this module will walk users through the creation, and running of a range of cyber-attacks on the cyber range	Workshops MOODLE	4	TCP/IP networking protocol, routing, switching fundamentals. Network security – design. Advanced system management (prevention)
Lesson learned from Cyber-MAR pilots: SCADA system in Port Container terminal	Management Technical Users E & R	Real life activities will provide to users a better understanding of risks targets attacks damages and remediation	Workshops MOODLE	1	OT and SCADA generic skills and knowledge

9 Analysis of course scores

Replies of attendees given before and after training sessions have been collected recorded and evaluated qualitatively

9.1 Questionnaire

The questionnaire used for assessment of awareness has been developed in different stages starting from a comprehensive literature review, selection of items by experts, elaboration of the various questions and checking their validity and comprehensiveness .Table 6 and Table 7 shows the questionnaires that have been prepared:

Table 6 - First Set of questions (A002) with correct answers

Questions	Autopsy is forensics tool that recovers (lots of) erased data, print system timeline events, extracts EXIF data	Techniques Tactics and Procedures (TTPs) …	The cyber « kill chain » was invented by Lockheed Martin in 2011 to « formalize » the potential phases of a (external) cyber-attack.	Computer & Network Forensics activities can be conducted (select all that apply)	Time inaccuracies will lead to problems or inconsistencies during analysis
correct answers	*TRUE*	*It can help understanding an attack and potentially identify the probable source of it*	*TRUE*	*In a reactive manner, when one is sure or probable a cyber-attack is occurring/has occurred, On a*	*TRUE*

				permanent basis (permanent hunt), In near real time or on past months	

Table 7 - Second Set of questions (A003) with correct answers

Questions	The Cyber-MAr cyber range has a network traffic capture feature	Volatility is a ...	Security Onion is a Linux distro for threat hunting, enterprise security monitoring, and log management	Kabana is a data visualization and exploration tool used for log and time-series analytics, application monitoring, and operational intelligence use cases.	Certutil command cannot be used to check the integrity of a file
Correct answers	*TRUE*	*tool for executing memory dumps*	*TRUE*	*TRUE*	*FALSE*

9.2 Results of the questionnaire

Green cells show correct answers.

Table 8 - A001 Test results pre- training

Autopsy is forensics tool that recovers (lots of) erased data, print system timeline events, extracts EXIF data	Techniques Tactics and Procedures (TTPs) ...	The cyber « kill chain » was invented by Lockheed Martin in 2011 to « formalize » the potential phases of a (external) cyber-attack.	Computer & Network Forensics activities can be conducted (select all that apply)	Time inaccuracies will lead to problems or inconsistencies during analysis	SCORE
TRUE	can help understanding an attack and potentially identify the probable source of it	FALSE	In a reactive manner, when one is sure or probable a cyber-attack is occurring/has occurred, On a permanent basis (permanent hunt), In near real time or on past months	TRUE	3/5
TRUE	can help understanding an attack and potentially identify the probable source of it	TRUE	In a reactive manner, when one is sure or probable a cyber-attack is occurring/has occurred	TRUE	5/5
TRUE	can help understanding an attack and potentially identify the probable source of it	TRUE	In a reactive manner, when one is sure or probable a cyber-attack is occurring/has occurred, In a preventive manner, to make sure everything is ok	TRUE	4/5
TRUE	gather victim host Information	TRUE	In a reactive manner, when one is sure or probable a cyber-attack is occurring/has occurred, In a preventive manner, to make sure everything is ok, In near real time or on	TRUE	3/5

Autopsy is forensics tool that recovers (lots of) erased data, print system timeline events, extracts EXIF data	Techniques Tactics and Procedures (TTPs) ...	The cyber « kill chain » was invented by Lockheed Martin in 2011 to « formalize » the potential phases of a (external) cyber-attack.	Computer & Network Forensics activities can be conducted (select all that apply)	Time inaccuracies will lead to problems or inconsistencies during analysis	SCORE
			past months		
TRUE	can help understanding an attack and potentially identify the probable source of it	TRUE	In a reactive manner, when one is sure or probable a cyber-attack is occurring/has occurred, On a permanent basis (permanent hunt), In near real time or on past months	TRUE	4/5
TRUE	can help understanding an attack and potentially identify the probable source of it	FALSE	In a reactive manner, when one is sure or probable a cyber-attack is occurring/has occurred	TRUE	3/5
TRUE	can help understanding an attack and potentially identify the probable source of it	FALSE	In a reactive manner, when one is sure or probable a cyber-attack is occurring/has occurred, In near real time or on past months	TRUE	4/5
FALSE	can help understanding an attack and potentially identify the probable source of it	TRUE	In a reactive manner, when one is sure or probable a cyber-attack is occurring/has occurred, In a preventive manner, to make sure everything is ok	TRUE	3/5

Table 9 - A001 Test results post- training

Autopsy is forensics tool that recovers (lots of) erased data, print system timeline events, extracts EXIF data	Techniques Tactics and Procedures (TTPs) ...	The cyber « kill chain » was invented by Lockheed Martin in 2011 to « formalize » the potential phases of a (external) cyber attack.	Computer & Network Forensics activities can be conducted (select all that apply)	Time inaccuracies will lead to problems or inconsistencies during analysis	Post Score
TRUE	can help understanding an attack and potentially identify the probable source of it	TRUE	In a reactive manner, when one is sure or probable a cyber-attack is occurring/has occurred, In a preventive manner, to make sure everything is ok, In near real time or on past months	TRUE	5 / 5
TRUE	can help understanding an attack and potentially identify the probable source of it	TRUE	In a preventive manner, to make sure everything is ok	TRUE	4 / 5
TRUE	can help understanding an attack and potentially identify the probable source of it	TRUE	In a reactive manner, when one is sure or probable a cyber-attack is occurring/has occurred, In a preventive manner, to make sure everything is ok	TRUE	5 / 5
FALSE	gather victim host Information	FALSE	On a permanent basis (permanent hunt)	FALSE	0 / 5
FALSE	gather victim host Information	FALSE	In a reactive manner, when one is sure or probable a cyber-attack is occurring/has occurred	FALSE	1 / 5
FALSE	are useful but should be taken with caution	FALSE	In a reactive manner, when one is sure or probable a cyber-attack is occurring/has occurred, In a preventive manner, to make sure everything is ok, On a permanent basis (permanent hunt), In near real time or on past months	FALSE	1 / 5

Table 10 Results A002 pre training

The Cyber-MAr cyber range has a network traffic capture feature	Volatility is a ...	Security Onion is a Linux distro for threat hunting, enterprise security monitoring, and log management	Kibana is a data visualization and exploration tool used for log and time-series analytics, application monitoring, and operational intelligence use cases.	Certutil command cannot be used to check the integrity of a file	**PRE Score**	**POST Score**
TRUE	tool for executing memory dumps	TRUE	TRUE	TRUE	4/5	4/5
TRUE	tool for executing memory dumps	TRUE	TRUE	FALSE	5/5	3/5
TRUE	tool for interpreting windows event logs	TRUE	TRUE	FALSE	4/5	5/5
FALSE	tool for analyzing pcap files	TRUE	TRUE	FALSE	3/5	NA

Table 11 Results A002 post training

The Cyber-MAr cyber range has a network traffic capture feature	Volatility is a …	Security Onion is a Linux distro for threat hunting, enterprise security monitoring, and log management	Kibana is a data visualization and exploration tool used for log and time-series analytics, application monitoring, and operational intelligence use cases.	certutil command can not be used to check the integrity of a file	Score
TRUE	tool for executing memory dumps	TRUE	TRUE	TRUE	4/5
FALSE	tool for executing memory dumps	FALSE	TRUE	FALSE	3/5
TRUE	tool for executing memory dumps	TRUE	TRUE	FALSE	5/5

10 Considerations about results

10.1 Data - A001

Analysis show that trends (Figure 5)in data from the tests collected are meaningful and did not happened by chance and Data (scores) are not dispersed

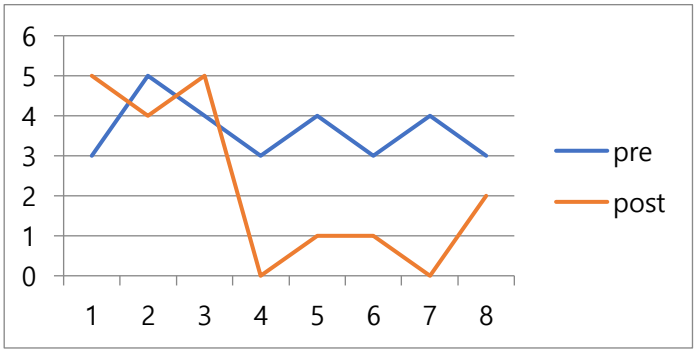

Figure 3 Graphic of scores (own elaboration)

Correlation between the two data sets (pre- training and post training) is 0.362738, this means that there is a medium correlation between the two data sets. At a first glance it appears that correlation should be improved though further or more effective training, however it is to be noted that people that

attended these courses were already enough skilled in the matter so that it is acceptable that the is not a lot of difference between pre an post raining results However these results suggest that the level of initial skillfulness of attendees affect the usefulness of training. Careful customization is necessary to get the maximum form the courses Variance of data for pre training data is 0.553571 and for post training data is 4.5 a relatively good value in relation to the composition of the classroom and the general knowledge about the matter to be taught.

Standard deviation measures how much variance there is in a set of numbers compared to the average (mean) of the numbers. Value is 0.744024 for pre training and 2.250926 for post training that is a better result.

10.2 Data A002

From the analysis it appears that trends in collected data are meaningful or did not happened by chance and Data (scores) are not dispersed.

However is to be noted that correlation between the two data sets is negative, i.e. -0.86603 that indicates a very weak correlation and that variables move in opposite direction. There may be an unknown factor still to be identified that influences both variables similarly. The relationship between this two data set can also change over time and may have periods of positive correlation as well.

Other data

Variance is 0.333333 for pre training and 1.00 for post training. As well-known s high variance tells that the collected data has higher variability, and the data is generally further from the mean. The second value is a bit high. It may well depend on the level of knowledge pre training and correct understanding during the course.

Standard deviation is 0.57735 for pre training and 1.00 for post training This latter value can be considered high.

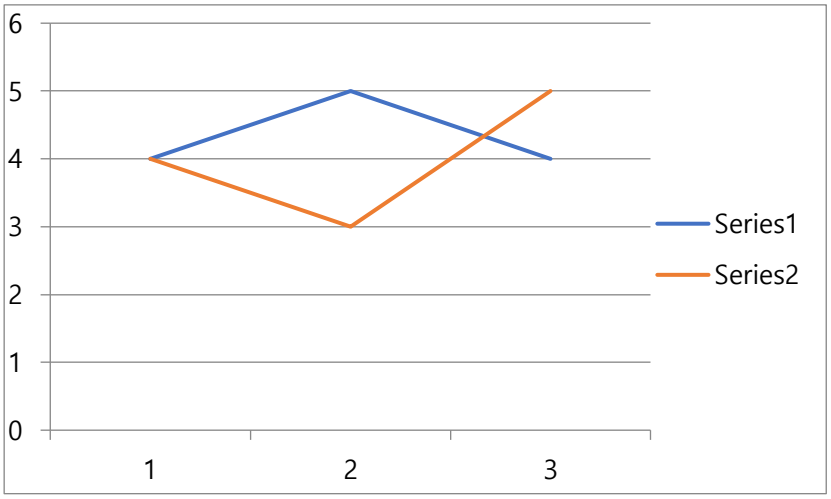

Figure 4 - A003 Score graphic (own elaboration)

11 Conclusions

To be really effective training and awareness needs be tailored to the appropriate levels of responsibility for different figures in the maritime community, both on board and ashore. To cope with the growing need to increase safety levels, it is necessary to create an awareness or training framework for personnel working in the maritime sector. Cyber range is the reply to these needs. Cyber range technologies and cyber ranges today are mature to be able to be efficiently employed.

Of course, it is necessary a good understanding of objectives, implementations and target achievements in order to avoid failed expectations and making investments that miss to achieve the expected return.

Cyber ranges, are an ideal tool for testing and validating the cybersecurity position of systems and software, as well as for training cyber defenders with the latest knowledge on cyber security tactics. Ranges help defenders to improve their cybersecurity skills with real-time drills on a secure version of their critical IT systems. They help organizations select, integrate and test new products and approaches without disrupting operations.

The potential of this approach and methodology is demonstrated by the first results of the Cyber-MAR training that shows how participants are able to to increase knowledge and awareness on security.

References

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. Safety Science, 131, 104908.

C. Onwubiko and A. Onwubiko, "Cyber KPI for Return on Security Investment," 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2019, pp. 1-8, doi: 10.1109/CyberSA.2019.8899375.

Canepa M., Hopcraft R. , Ballini F., & Karamperidis S. . (2021). Cyber awareness raising - an integrated maritime cyber risk management approach. International Association of Maritime Economists (IAME) 2021 Conference 'Accelerating Transitions' (IAME 2021), Rotterdam. Zenodo. https://doi.org/10.5281/zenodo.6346898

Canepa, M., Ballini, F., Dalaklis, D., & Vakili, S. (2021, March). Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain. In Proceedings of INTED2021 Conference (Vol. 8, p. 9th).

Home - CyberMAR [online]. (no date-b). CyberMAR. [Viewed 22 June 2022]. Available from: https://www.cyber-mar.eu/

Dalaklis, D. & Schröder-Hinrichs, J.U. (2019). 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

ECSO - European Cyber Security Organisation. [Viewed 21 June 2022]. Available from: https://www.ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf

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

Gordon, L. , Loeb, M. and Zhou, L. (2016) Investing in Cybersecurity: Insights from the Gordon-Loeb Model. Journal of Information Security, 7, 49-59. doi: 10.4236/jis.2016.72004.

Gordon, L. A. and M. P. Loeb, 2002, "The Economics of Information Security Investment," ACM Transactions on Information and System Security, pp. 438-457

Hatzivasilis, G. et al. (2020) Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. Applied Sciences. [Online] 10 (16), 5702. [online]. Available from: http://dx.doi.org/10.3390/app10165702.

Hautamäki, J., Karjalainen, M., Hämäläinen, T., & Häkkinen, P. (2019). Cyber security exercise: Literature review to pedagogical methodology. In INTED Proceedings (No. 2019). IATED Academy.

Home - CyberMAR [online]. (no date). CyberMAR. [Viewed 21 June 2022]. Available from: https://www.cyber-mar.eu/

Inan, C. A Visual Tool for the Analysis of Cybersecurity Investments.

Introduction to Return on Security Investment [online]. (no date). ENISA. [Viewed 21 June 2022]. Available from: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment

Koziol, J., (2022b). Cybersecurity Awareness: What It Is And How To Start [online]. Forbes Advisor. [Viewed 21 June 2022]. Available from: https://www.forbes.com/advisor/business/what-is-cybersecurity-awareness/

Losi, S 2006, "The ROI of Security." Security Matters, Software Engineering Institute, Carnegie Mellon University, http://www.sei.cmu.edu/library/abstracts/news-at-sei/securitymatters200605.cfm

McDaniel, Lucas, Erik Talvi, and Brian Hay. "Capture the flag as cyber security introduction." 2016 49th hawaii international conference on system sciences (hicss). IEEE, 2016.

Poole, E., (no date). Quantifying Business Value of Information Security | SANS Institute [online]. Cyber Security Training | SANS Courses, Certifications & Research. [Viewed 21 June 2022]. Available from: https://www.sans.org/white-papers/33149/

R. Beuran, D. Tang, C. Pham, K. Chinen, Y. Tan, Y. Shinoda, "Integrated Framework for Hands-on Cybersecurity Training: CyTrONE", Elsevier Computers & Security, vol. 78C, June 2018, pp. 43-59.

Rowe, Brent & Gallaher, Michael. (2006). Private sector cyber security investment strategies: An empirical analysis.

Somarakis, Iason & Smyrlis, Michail & Fysarakis, Konstantinos & Spanoudakis, George. (2020). Model-Driven Cyber Range Training: A Cyber Security Assurance

Perspective. 10.1007/978-3-030-42051-2_12.

Stopford, M., (2008). Maritime Economics 3e. Taylor & Francis Group.

Tam K. et al. (2021) The potential mental health effects of remote control in an autonomous maritime world, Journal of International Maritime Safety, Environmental Affairs, and Shipping, 5:2, 40-55, DOI: 10.1080/25725084.2021.1922148

Tam, K., Moara-Nkwe, K., & Jones, K. D. (2021). The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training. Maritime Technology and Research, 3(1), 16-30.

The technological aspects of digital transformations: this is what BCG Platinion is about [online]. (no date). Italy - IT. [Viewed 21 June 2022]. Available from: https://www.bcg.com/it-it/beyond-consulting/bcg-platinion/default

V. E. Urias, B. Van Leeuwen, W. M. S. Stout and H. W. Lin, "Dynamic cybersecurity training environments for an evolving cyber workforce," 2017 IEEE International Symposium on Technologies for Homeland Security (HST), 2017, pp. 1-6, doi: 10.1109/THS.2017.7943509.

What is a Cyber Range? | CYBERWISER.eu [online]. (no date). CYBERWISER.eu | Cyber Range & Capacity Building in Cybersecurity. [Viewed 21 June 2022]. Available from: https://www.cyberwiser.eu/content/what-cyber-range

Willemson, J. (2010). Extending the Gordon and Loeb Model for Information Security Investment. 2010 International Conference on Availability, Reliability and Security, 258-261.

Wilson, M. and Hash, J. (2003), Building an Information Technology Security Awareness and Training Program, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151287 (Accessed June 21, 2022)

Yamin, M.M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Comput. Secur., 88.