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

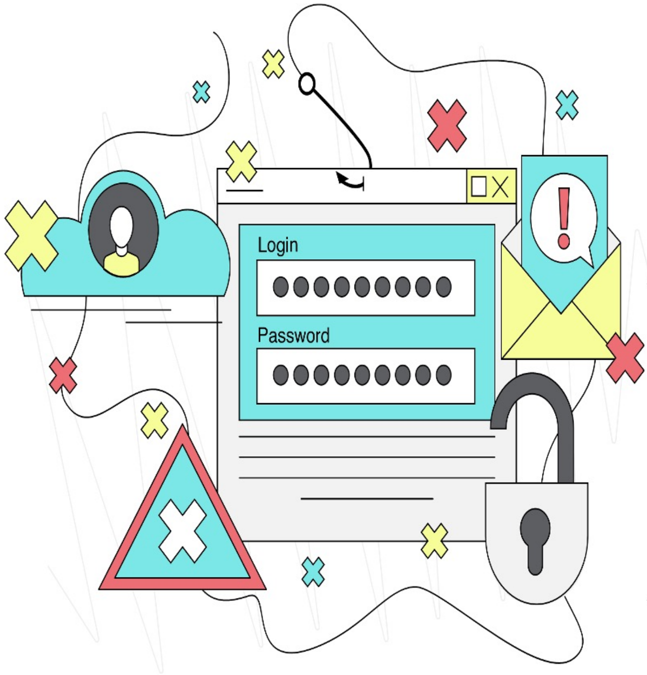
IAME CONFERENCE 2022
INTERNATIONAL ASSOCIATION OF MARITIME ECONOMISTS

Presenter: Dr. Canepa Monica
World Maritime University

AGENDA

1. **Challenges in cyber risk management education and training in maritime sector**
2. **Implications of a Maritime Cyber incident**
3. The human factor in Cyber Safety Management (focus in Maritime sector)
4. Training as a Cyber Risk Management Approach: Cyber-MAR training and cyber ranges

INTRODUCTION (REVIEW)



The maritime sector remains one of the most important financial sectors for the European economy. Acting as the backbone of world trade, around 80% of world trade in goods is carried by the international shipping industry domain and is in full growth .

Maritime information systems, whether on board ships or in ports, are numerous, built with standard components available on the market and in many cases designed without accounting for the cyber risk, which is ever growing.

Digitization in the maritime logistic domain is one of the driving factors towards its growth. However, the growing digitization of the maritime value chain actors increases the attack surface of maritime information systems.

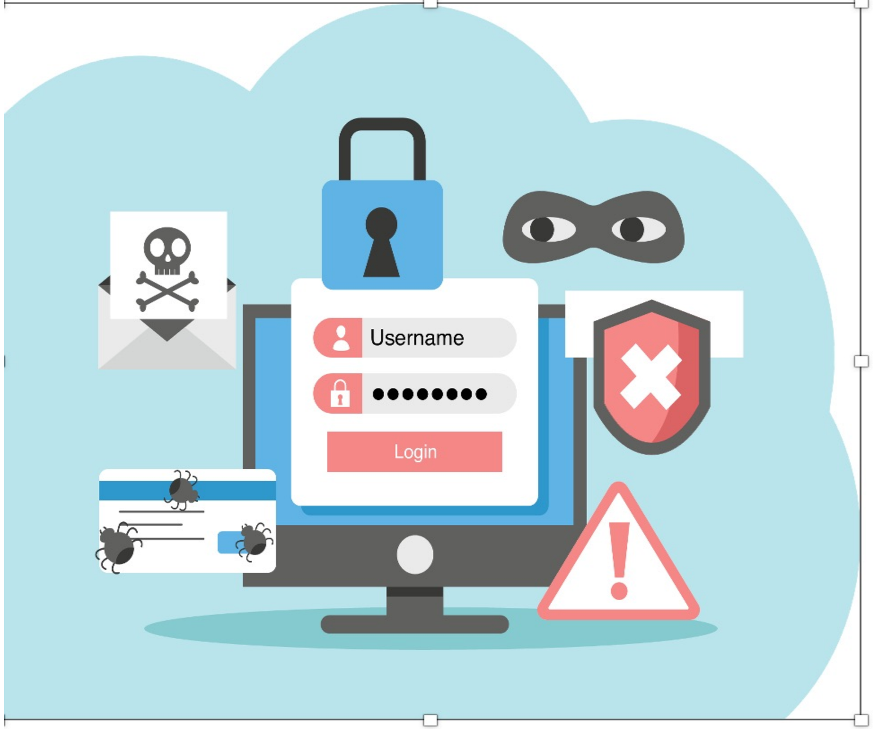
ACCIDENTS

Two most known cases of cyber-attacks with devastating financial and societal impacts in shipping industry

The Maersk Case**:** In June 2017, the NotPetya malware, hit shipping giant A.P. Moller-Maersk, which moves about one-fifth of the world's freight. Operations at Maersk terminals in four different countries were impacted, causing delays and disruption that lasted weeks. According to a statement issued by the company, the total cost for dealing with the outbreak landed somewhere in the $200 to $300 million range

The Antwerp Port Case**:** Hackers working with a drug smuggling gang infiltrated the computerized cargo tracking system of the Port of Antwerp to identify the shipping containers in which consignments of drugs had been hidden. The gang then drove the containers from the port, retrieved the drugs, and covered their tracks. The criminal activity continued for a two-year period from June 2011, until it was stopped by joint action by Belgium and Dutch police.

Vulnerability of maritime industry to the cyber risks



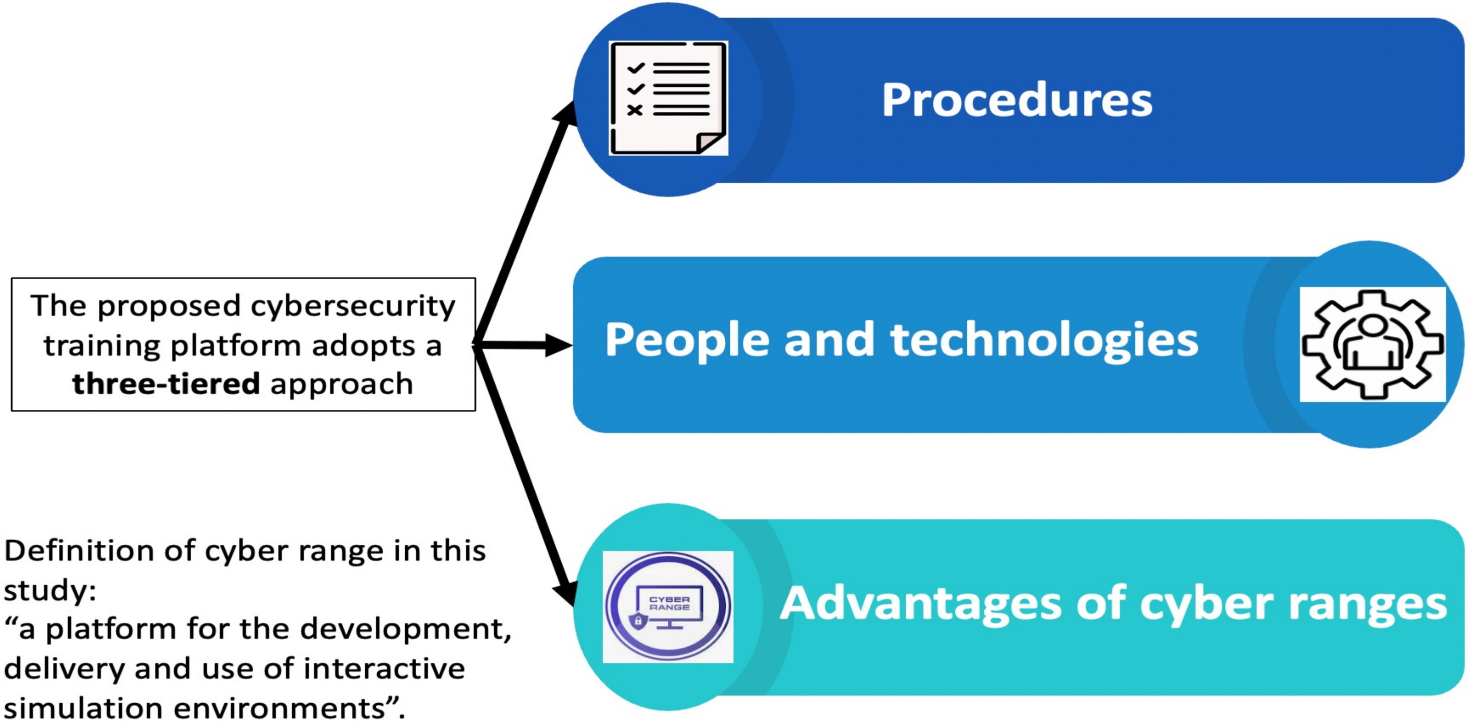
The lack of awareness about cyber threats is evident in several different business sectors, including the maritime sector.

AIM & OBJECTIVES

The aim of the research is to 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.

DATA/METHODOLOGY



The proposed cybersecurity training platform adopts a **three-tiered** approach

Procedures

People and technologies

Advantages of cyber ranges

Definition of cyber range in this study:
“a platform for the development, delivery and use of interactive simulation environments”.

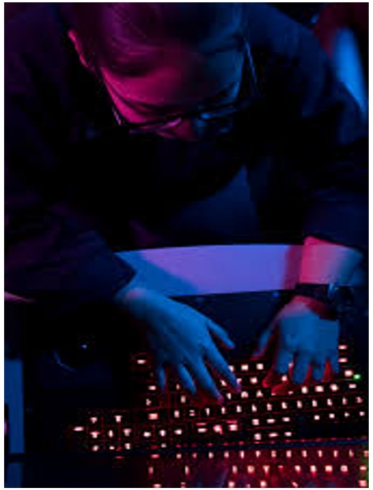
METHODOLOGY

Deployment of three-tiered approach can result in:

Train people: Cyber security professionals and employees in other key-areas either directly or indirectly connected with cybersecurity need to receive continuous training to be well prepared when an attack occurs.

Test technologies: Such a platform offers the opportunity to test technologies in a secure environment. Apart from its training role, the tool can act as a virtual testbed of novel technologies prior to their introduction in production.

Measure procedures: By deploying a novel cyber range-based platform possible areas for improvement in established procedures can be extracted in a realistic, cost and time-efficient efficient manner without the risk of business disruption.



Cost-Effectiveness Studies

Evaluation of investment

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.

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.

ROI in cyber security or Return on Security Investment allows companies to measure the KPIs (Key Performance Indicators) of the projects.

Basics of the Cyber Risk Management approach

Risk based approach

- Assessment and identification of the highest risk areas
- Establishment of a priority list
- Proper resource allocation plan
- Inclusion of identified cyber risks in the organizations business risk management

Initial considerations on weakness

- Attacks are on the rise
- Humans are considered a weakness in an organizations cybersecurity
- Providing basic training is not enough to educate employees

A cost-effective approach to cyber security

- training
- Awareness raising

Cyber-Mar project

The expected main results are the following:

Ensure that cyber-security and IT professionals can easily create scenarios of cyber-attacks (past or recently emerging) and/or insert data and logs from historical, current or fictional cyber-attack incidents in a straightforward manner.

Easy integration to low-level parts of the port and shipping systems (down at the level of sensors or PLCs), thus the actual effect on the real and operating environment may be estimated.

The platform will be its interoperability of different cyber-range systems, professionals will have the opportunity to detect attacks on collaborating. organisations' systems and thus be able to fail-safe their own, not allowing for cascading effects to take place.

Development of training

Cyber-MAR Training Levels

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

Cyber-MAR 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

INTEGRATED MARITIME CYBER RISK APPROACH

Enhance the **capabilities** of cybersecurity professionals and **raise awareness** on cyber-risks

Deploy Cyber-MAR Range, training modules through LMS, improvement in response times in specific resilience metrics

Assess cyber-risks for operational technologies (OT)

Maritime Cyber-Risk Assessment deployment and integration in Cyber-MAR platform

Quantify the **economic impact** of cyber-attacks across different industries with focus on **port disruption**

Quantify economic risk in terms of Time-to-Recover or Product Value at Risk, integration in Cyber-MAR platform

RESULTS

The econometric model developed would be used as first of risk assessment framework for quantifying the impact from cyber-attack of the maritime domain.

To cope with the growing need to increase safety levels, it is necessary to create an   a wareness 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.

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.

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.

IMPLICATIONS FOR RESEARCH

Identification of the main gaps in maritime cyber security coupled with the training and awareness needs on cyber security aspects.

As mentioned in various reports on cyber preparedness "There's no substitute for preparedness".

Preparedness measures act as the umbrella that covers end to end the system and is fully operating even during the incident time. In effect, the preparedness level does not differ even when an incident happens.

Thank you for your attention.

WORLD MARITIME UNIVERSITY

Monica Canepa

✉ moc@wmu.se

Cyber MAR

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement No. 833389