Grant Agreement Number: ***833389***

Project acronym: Cyber-MAR

Project full title: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389. The content of this document reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information it contains.

COURSE: **Using a Cyber Range to Understand risk**

DELIVERY DATE: 1st December 2021

COURSE DESCRIPTION: The training course is designed to provide a high-level overview of the Cyber Range as a tool to understand cyber risk through the exploration of the insights that can be gained by running scenarios on the cyber range: Econometric models and Remediation Plans
This course is intended to equip an understanding of how to plan for cyber range scenarios application to cyber risk management.
The intended audience is managers who want/have to use the cyber range capabilities to elaborate scenarios for risk analysis and training.
The objective is to make learners plan scenarios for risk analysis and insights on the cyber range.

This training's intended audience is IT, cyber security, and OT personnel.

DELIVERY MODALITY: E-LEARNING CLASS

DURATION: 1,5 hours

Syllabus

Online Training "Using a Cyber Range to Understand risk"

INTERMEDIATE LEVEL

©Cyber-MAR Consortium 2019-2022

PREREQUISITE: Cyber risk management proficiency, deep knowledge of IT systems and networks architecture, knowledge of IT/OT infrastructures pertinent to shipping and ports activities

CONTENTS

1. Cyber-Risk Modelling
    1.1. Overview of the Main Stages in the Risk Modelling Process
    1.2. Cyber-Risk Assessment
    1.3. Risk Modelling and Analysis
        1.3.1. Introduction, Purpose, and Usefulness
        1.3.2. MaCRA framework for risk modeling and analysis
        1.3.3. MaCRA Graphs (incl. MaCRA graph features for analysing dynamic risks and communicating assessment uncertainties)
2. Cyber-Risk Impact Assessment
    2.1. Overview of Risk Impact Assessment
    2.2. Use of Port Operations Models for estimating cyber-risk impacts
    2.3. Port Performance (measuring and assessing critical effects on port performance)

✓ Final Training evaluation

TRAINING STRUCTURE

The training will be delivered online through zoom.
The attendees will receive an invitation zoom link to join the training.

LEARNING OUTCOMES

The participants will develop knowledge and skills necessary to apply the principles of:

- Remain aware of evolving technical infrastructures
- Use critical thinking to analyze organizational patterns and relationships

©Cyber-MAR Consortium 2019-2022

- How to use network analysis tools to identify vulnerabilities
- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications
- packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump)
- Network mapping and recreating network topologies
- Organization's risk tolerance and/or risk management approach
- Information security program management and project management principles and techniques
- Risk Management Framework (RMF) requirements
- Cybersecurity and privacy principles are used to manage risks related to the use, processing, storage, and transmission of information or data
- Specific operational impacts of cybersecurity lapses
- Risk management processes (e.g., methods for assessing and mitigating risk)

©Cyber-MAR Consortium 2019-2022