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

Syllabus

Training level 1 (Entry level)

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: **Cyber MAR - ENTRY LEVEL - LMS**

DELIVERY DATE: 24th – 26th November

COURSE DESCRIPTION: 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.

STUDENT LEARNING OUTCOMES: participants will be able to make an active part in the process of detecting and responding to attacks.

DURATION: E-LEARNING CLASS **9 Hours**
WORK OUT CLASS **3 Hours**

MODULE 1: **Intro and scenarios**

Introduction of Cyber MAR project and actors involved

Value of data

Data, seaside and internet connections

The use of data

Meaning of network (wired and wireless)

Ships environments

People involved

SCADA meaning with samples

Responsibilities

Range of ships – open discussion

Assets on board (sat, ecdis, wireless, crew, …)

Kind of attacks USB

Kind of attacks Internet

Kind of attacks spoofing and jamming (basic)

Kind of attacks DOS

Kind of attacks misinformation

Kind of attacks social engineering (basic)

Data Theft and/or leak

Economic reasons

Revenge reasons

The role of Cyber Range

Network basics

Ships and Boat

MODULE 2: **The Regulatory Framework for Cyber Security in Critical Infrastructures"**

IMO approach

EU Law - Framework of transport infrastructure resilience

MODULE 3: **Attacks issues in deep**

Content: wifi, sat, spoofing, jamming, dos, misinf, social engineering, data theft, SCADA.

MODULE 4: **Mitigation and remediation**

Mitigation follows “Attack issues in deep” schema (module 3)

MODULE 5: **Mini-master on cyber security – Entry level**

Cybersecurity in real-life

Hacking, cybercrime & cyber espionage

Security awareness

MODULE 6: **Overview of real cases**

What happened?

Why?

How to avoid it

MODULE 7: **Conclusions and intro to the next level**

The reason for of cyber range

Intro to second level training

- Required skills
- How does it work and why
- Deep dive into level one schema

Final Training evaluation