International Association of Maritime Economists (IAME) 2021 Conference 'Accelerating Transitions'

29 June - 02 July 2021

Submission ID : RTM175

Cyber awareness raising - an integrated maritime cyber risk management approach

Submission Topic : Ports_Cyber Security in Ports

Submission Status : Pending Review

Research Method(s): The study is conducted based on the EU Cyber-MAR platform where will be simulated a cyber attack in a port system, using other case studies to illustrates the impacts of disruptions.

Research Data: The data to analyze will be got from a port pilot action implemented and from the other cases above mentioned.

Expected Results: The paper will argue that to reduce the impacts of a cyber-incident, port stakeholders must adopt a hybrid training approach when managing cyber-risk. Cyber awareness training provides a cost-effective, and practical risk management approach, which not only reduces the likelihood of an incident occurring but also reduces the impacts of one if it does.

Keywords: Cyber awareness raising, Maritime cyber risk management approach, Hybrid training apporach , ,

Preference For Submission: Full paper

Monica Canepa [1] *

Email : moc@wmu.se, **Status :** Published

Rory Hopcraft [2]

Email : rory.hopcraft@plymouth.ac.uk, **Status :** Published

Submission Summary : Ports and their stakeholders are highly interconnected within dynamic maritime supply chains. Managing these networks has led to an increasing dependence on information and communication technologies (ICT), opening up the sector to new vulnerabilities from cyber-risks. Cyber risk management is currently a major challenge for the maritime sector. Maritime information systems are often built with off-the-shelf components, which in many cases are designed without considering the cyber risks that these introduce to the wider system. Training has long formed part of the maritime sector's risk management approach. Much of the current cybersecurity legislation explicitly mentions training as a way to help secure the maritime sector's digital infrastructure. As ports form the nexus between land and sea it is crucial that they prioritize cybersecurity training as a risk management strategy to ensure the continued security of maritime information systems. This paper will demonstrate, using the EU Cyber-MAR platform, the disruption caused by a spear-phishing attack targeting a port's power management network. The paper will discuss the financial implications that this attack, and larger-scale cyber-incidents, could have at a corporate level (reputation, contracts, fines), as well as at an EU level (large scale disruption).