IAME 2021
ROTTERDAM

Cyber Awareness Raising – An Integrated Maritime Cyber Risk Management Approach

Presenter: Dr Stavros Karamperidis, University of Plymouth

Research team: *R Hopcraft[1], M Canepa[2], S Karamperidis[1], F Ballini[2]*

[1] University of Plymouth, [2] *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

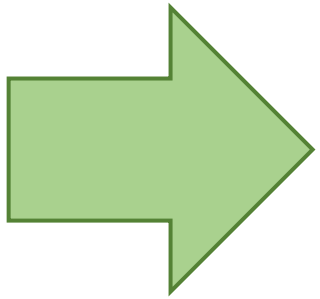
Challenges in cyber risk management education and training in maritime sector

- Lack of cybersecurity educators,
- Low interaction with the industry,
- Little understanding of the labour market,
- Outdated or unrealistic platforms in education environments,
- Difficulties in keeping pace with the outside world

IAME 2021
ROTTERDAM

Cyber-security awareness in port

- Many ports implements processes of automation, in terms of:
  - Information technology (IT)
  - Operational technology (OT)
- This new technology is designed to increase efficiency the profitability of operations



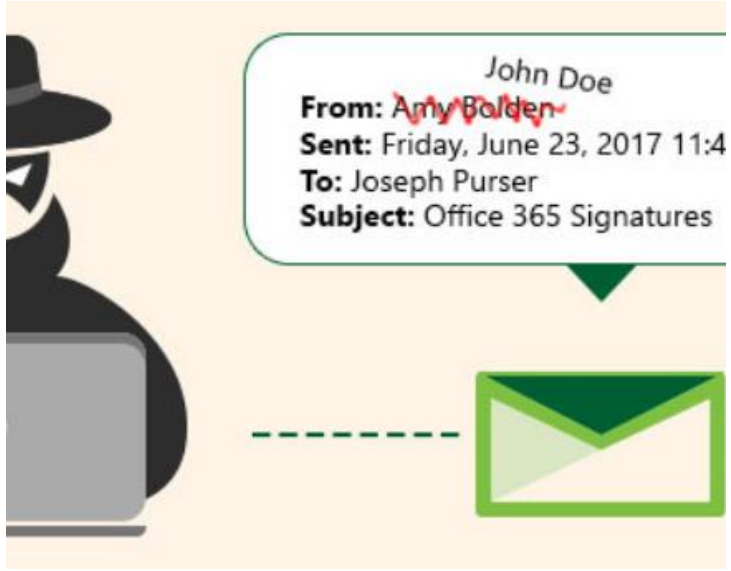
The sector is now finding itself increasingly open to cyber risks

The management cyber risks have gained increased attention at both national and international levels:

- *IMO published Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management System*, which formalized the need to address cyber risk in the maritime sector (2017)
- The European Union, through the NIS Directive highlights the importance that the maritime sector has on national and global trade. States should be working with key stakeholders within the industry to ensure that these essential services remain safe and secure
- The EU ratified the *General Data Protection Regulation (GDPR),* which stipulates that companies that fail to ensure the security of personal data they hold are liable to pay considerable fines of up to €20,000,000 or 4% of global annual turnover. GDPR breach can have serious financial implications

IAME 2021
ROTTERDAM

Implications of a Maritime Cyber incident



The scenario chosen was a **malicious email**

The malware can propagate through all parts of the ports IT systems allowing an attacker to control the power management system remotely

Such a scenario will have an impact on the port's profitability

Based on the Port of Valencia (PoV) these impacts would include the:

- loss of power to the cranes across the port
- reducing the ability for the port to unload/reload ships
- move containers through the port
- move goods onwards towards their destination
- loss of administrative systems, where digital manifests and logs become inaccessible

Implications of a Maritime Cyber incident

Goods handled by PoV are split in two categories:

1. non-time critical (high volume and low value such as construction materials)
2. time critical (low volume high value goods): Spain has the highest production share of Oranges (54%), small citrus fruit (67%), avocados (91%), among others, in Europe

Delays, or damage to the refrigerator units, caused by the cyber-incident affecting the power supply, could have a catastrophic impact to the port!

Impact in terms of litigation, reputation and monetary

The impact of the damage could be spread to the overall Spanish economy

Needing to travel to another port would extend the shipping time of products

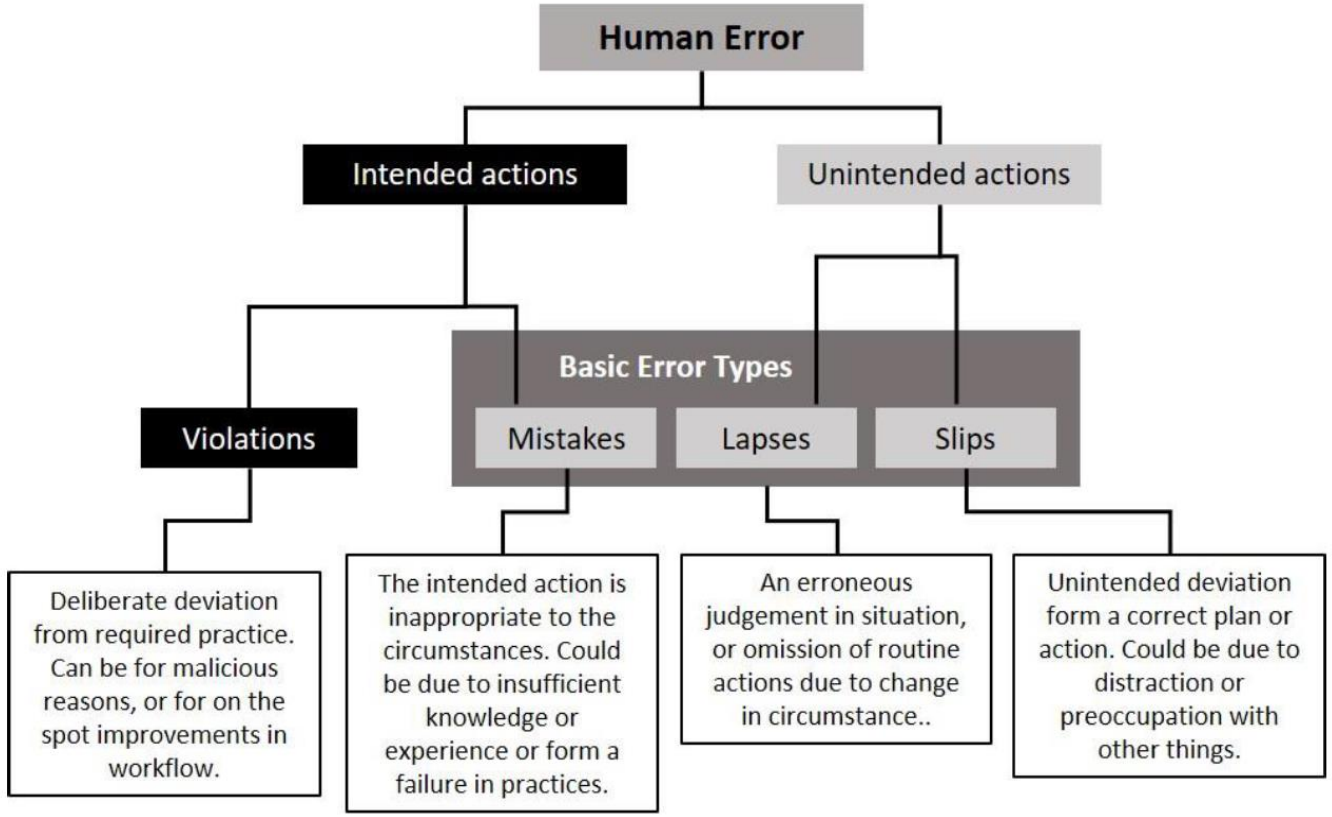
Other ports will still be servicing their normal operations, leaving limited capacity

Other consequences…

- **cost to replace, or repair equipment damaged during the incident**
- **financial impact on the company, both in the short and long term**
- **damage of customer confidence and the loss in market share**

The consequences of a cyber-incident will not be limited to a single company (e.g. PoV)

The human factor in Cyber Safety Management



Source by Barnett, M. L. (2005) 'Searching for the Root Causes of maritime Casualties', WMU Journal of Maritime Affairs, 4(2), pp. 131-145.

The maritime sector has always relied upon human involvement from sailing the ships to operating the port cranes

Each personnel will have a different role to play in safety

The human element is referred to as the biggest internal threat facing the cybersecurity of companies

Verizon Data Breach Investigations report asserts that 30% of reported data breaches involved internal actors, and that 22% of all breaches were caused by human error (not following good cyber risk management practices)

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

Humans play important role in the safety of system, and the importance on ensuring they attain the right skills and knowledge to perform their safety function

IAME 2021
ROTTERDAM

The human factor in Cyber Safety Management: focus in Maritime sector

- In 1993 IMO argue that safety is based on many complex interacting variables **including training, skill level and experience (right skills)**
- Over the last decade is the IMO's drive to place **the human element at the centre of the safety management discussion**. This placement was achieved through the introduction of the *International Management Code for the Safe Operations of Ships and for Pollution Prevention (ISM Code)*
- The restructuring of the role of the human element in safety management ensures that **personnel are equipped with the right skills to recognize when unsafe operations** could be occurring and proactively respond to them
- As a part of the ISM Code companies should develop and implement a *safety management system (SMS*). Companies **should include instructions and procedures to ensure the safety operation of ships** that is compliant to international regulations and guidance. **Personnel should be able to carry out the safety processes and practices outlined**
- The IMO also uses the *International Convention on Standards of Training and Watchkeeping*, to highlight the safety role personnel play. **Companies are obligated to consider their operation-specific safety requirements and ensure their personnel can demonstrate appropriate skills to fulfil them**

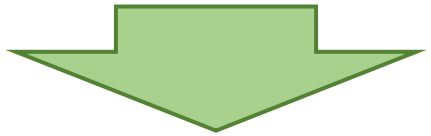
The human element has demonstrated both its ability to be a weakness and strength in the management of cyber risk

Focus should be given to developing the human element's ability to implement cyber risk management processes, as a way to compliment the technical and procedural mitigations

IAME 2021
ROTTERDAM

Training as a Cyber Risk Management Approach

- Cyber awareness training offers a cost-effective and meaningful cyber risk management approach (reduce system vulnerabilities and the potential loss)
- *Lack of cybersecurity educators, low interaction with the industry, little understanding of the labour market, outdated or unrealistic platforms in education environments, and difficulties in keeping pace with the outside world*



Making the implementation of quality cyber security training challenging

There are many compelling reasons why cyber training should be implemented as a risk management practice:

1. **Attacks are on the rise as more employees are working from home**
2. **Humans are a considered a weakness in an organization's cybersecurity**
3. **Compliance requirements for businesses and operations are increasingly focused on employee training**
4. **Providing basic training once is not enough to educate employees**
5. **Anyone can become the victim of a phishing attack**

Training as a Cyber Risk Management Approach

- *ISO, through ISO31000:2009* – Risk Management – Principles and Guidelines reiterates the importance of implementing adequate training sessions and programs to ensure that personnel are able to adhere to risks management strategies
- *ISO/IEC27001:2013* – Information Technology – Security Techniques applies the risk management logic to cybersecurity to achieve compliance all personnel shall receive appropriate awareness, education, and training on information security that is relevant to their job role
- *BIMCO's Guidelines on Cyber Security Onboard Ships* training should cover a broad level of cybersecurity activities
- *Resolution MSC.428* the IMO has drawn a clear link between the development of maritime cyber awareness skills and cyber risk management.
- *The ISM Code:* "Company should establish and maintain procedures for identifying any training which may be required in support of the SMS and ensure that such training is provided for all personnel concerned". The training will provide personnel with the skills required to ensure they do not compromise the safety or security of the systems they operate

There is no explicit guidance on what cyber awareness competencies should consist of

- The IMO recommends companies utilise the *NIST Cybersecurity Framework*. The NIST Framework highlights awareness and training as one of the fundamental elements of the Protect function. In addition, the NIST Framework drives companies to develop cyber risk management practices that are both ***relevant and cost-effective.***

IAME 2021
ROTTERDAM

Training as a Cyber Risk Management Approach: cyber ranges

Training increases in effectiveness if it is able to **simulate situation that may occur in the respective organizations** day-to-day operations

They are **considering the implications of their actions** on other parts of the network, ensuring they do not inadvertently compromise the safety or security of another system

Cyber Range: trainees access a simulated network environment in which they can practice and improve their skills

Includes the **simulation of attacks**, of users and of their activities and of any other Internet, public or third-party services that the simulated environment may depend upon

Cyber Ranges offer the capability to employ tools, attacks and procedures **safely without risk** to the organization's digital infrastructure

Cyber ranges are one of the best ways to run real attack scenarios and immerse the team in a live response exercise

IAME 2021
ROTTERDAM

Training as a Cyber Risk Management Approach: Cyber-MAR training

Studies show that the use **of multiple methods of training** produced the **highest correlation to perceived security effectiveness in employees**

The Cyber-MAR project aims to develop an **“innovative cybersecurity simulation environment for accommodating the peculiarities of the maritime sector”**

Through the analysis of data collected from EU member states CSIRTs/CERTs, the project will provide a knowledge-based platform to aid cyber risk management decisions

It is important to consider the **level of responsibility each personnel** has for risk management

EU’s Cyber-MAR levels: each personnel receives the most appropriate training

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

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

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 material reflects only the authors’ view and the European Commission is not responsible for any use that may be made of the information it contains.

IAME 2021 ROTTERDAM

THANK YOU FOR YOUR ATTENTION

IAME 2021
ROTTERDAM