



GREENPORT
Alliances



Co-funded by
the European Union

COURSE NAME: Sustainable Maritime Operations and Green Ports

Module 10 (Week 10)

Lecturer

Lecturer contact info:

SECURITY PROCEDURES AND CRISIS MANAGEMENT IN A DIGITALIZED ENVIRONMENT



GREENPORT
Alliances



Co-funded by
the European Union

1. Introduction

- Although **digitization** offers enormous benefits, it also widens the maritime industry's exposure to **cyber risks**, creating a wider surface for attacks
- **Cyber incidents** can result in **loss of life**, **loss of control** over ships or sensitive data, as well as **hijacking** of ships and/or cargo
- Effective **security procedures** and **robust crisis management** are fundamental aspects of maritime safety, environmental protection and business continuity



2. Security procedures for digitalized systems

- The integration of **information technology (IT)** and **operational technology (OT)** systems presents a major vulnerability, as many shipboard OT infrastructures are older, designed for functionality rather than cyber resilience, and often lack basic security controls such as encryption or regular updates
- This leaves critical systems, such as navigation and propulsion, vulnerable to attacks such as **GPS spoofing**, **ransomware** and **malware injection**



2. Security procedures for digitalized systems

- Efficiency gains from digitalization, such as **real-time tracking** and **reduced downtime**, are directly linked to increased **exposure to cyber threats**
- This creates a **crucial balance** that requires **proactive risk management** rather than reactive responses
- The full realization of efficiency and sustainability benefits depends on the **effective management of these new cyber risks** – maritime operations cannot fully benefit from digitalization without a simultaneous and significant investment in **robust cybersecurity**

2. Security procedures for digitalized systems

- International organizations such as **IMO** and **BIMCO** have developed **guidelines for cyber risk management in the maritime sector**
- The **IMO Cyber Risk Management Model** defines the process of identifying, analyzing, assessing and communicating cyber risks and their acceptance, avoidance, transfer or mitigation to an acceptable level
- **BIMCO's guidelines** for cyber security on ships offer a practical five-step approach: **identification, assessment, protection, detection, response and recovery**

2. Security procedures for digitalized systems

- Effective implementation of maritime cybersecurity requires a strategic and layered approach, known as “defense in depth and breadth”
- This involves a combination of protective and detection layers, from the physical security of the ship to network protection and intrusion detection, through periodic scanning and testing: **segmenting networks, regular penetration testing and vulnerability assessments, advanced threat detection tools**

3. Crisis management and emergency response

- In a digitized maritime environment, **effective crisis management and emergency response** is critical to minimizing the impact of cyber incidents and ensuring business continuity
- **Crisis management plans** must include strategies for rapid detection, containment, eradication and recovery from cyberattacks
- IMO's cyber risk management guidelines recommend that organizations have **clear incident response and recovery strategies**

3. Crisis management and emergency response

- This includes **establishing procedures for collation and retention of security records and periodic review by competent personnel as part of routine operational maintenance**
- An important aspect is also the establishment of an **anonymous cyberattack reporting system** to improve transparency in risk management and enable the generation of unique evidence on risk assessment and mitigation
- It is critical that companies establish an **internal threat team** to assess new threats and regularly update response plans



3. Crisis management and emergency response

- This includes **establishing procedures for collation and retention of security records** and **periodic review by competent personnel** as part of **routine operational maintenance**
- An important aspect is also the establishment of an **anonymous cyberattack reporting system** to improve transparency in risk management and enable the generation of unique evidence on risk assessment and mitigation
- It is critical that companies establish an **internal threat team** to assess new threats and regularly update response plans

3. Crisis management and emergency response

- **Proactive planning** and **regular testing of incident response protocols** are key to minimizing impact and ensuring rapid recovery
- **Regular drills** and **crisis simulations** are essential for testing response plans, ensuring that damage is minimized and recovery is rapid when an attack occurs
- Lack of coordination before and during crises, unclear notification procedures, and inconsistent communication between government and private actors can **hinder crisis response**

4. Human factors and crew management

- Digitalisation and automation are redefining the role of the human, requiring **new competencies beyond traditional maritime skills**
- IMO emphasises that the **human element** must be considered when reviewing, developing and implementing new and existing requirements, including skills, education and training, and human capabilities, limitations and needs
- The move towards **autonomous and remotely operated processes** is changing the structures of organisations and the way people work, introducing new safety challenges that affect crew and shore-based personnel

4. Human factors and crew management

- This means that safety in modern shipping increasingly relies on system robustness, resilience and the ability to continuously improve through the dynamic **interaction between human, organisational and technical factors**
- **Training and awareness programs** are essential to ensure that crew and shore-based personnel are equipped to cope with a digitalized environment
- **Effective cybersecurity training** for seafarers is not just about acquiring technical skills, but also fostering a culture of constant vigilance and responsibility

4. Human factors and crew management

- Courses such as “**Maritime Cyber Security Awareness for Seafarers**” cover the definition of cybersecurity, existing cyber threats, vulnerabilities in shipboard IT and OT systems, and mitigation and defense measures
- These courses emphasize that cybersecurity is everyone’s responsibility and must be integrated into the **safety/security management system (SMS)**
- In addition to technical skills, digital maritime learning offers interactive, short courses that address specific skill gaps, including **crew familiarization training, operational and emergency training, and troubleshooting training**

4. Human factors and crew management

- The use of technologies such as **virtual reality (VR)** and **digital twins** can enhance crew competencies by allowing them to familiarize themselves with vessels and practice operations in a safe, virtual environment
- „**Operational skills**“, "**digital skills**" and "**maritime competence**" as the most important skills and competencies for maritime autonomous surface ship (MASS) operations
- **Interpersonal skills**, such as communication, collaboration, teamwork, adaptability, leadership and emotional intelligence, are **critical** to aligning different interests and ensuring harmonious operations



4. Human factors and crew management

- **Human-machine interaction** in the maritime sector is becoming increasingly complex with the introduction of **automation** and **artificial intelligence**
- In **ports**, semi-automation offers a middle ground between full automation and traditional human-operated systems, where machines perform repetitive or hazardous tasks, while human workers continue to supervise operations and make complex, high-risk decisions
- This **hybrid strategy** is designed to increase efficiency and create a safer, healthier and more environmentally friendly work environment

5. Conclusion

- **The key insight is that the full potential of digitalization can only be realized through proactive and comprehensive cyber risk management, integrated into all aspects of maritime operations and safety management**
- **This implies a shift from mere compliance with regulations to building a resilient cyber security culture**
- **This includes continued investment in advanced security technologies, the development of robust incident response and business continuity plans, and comprehensive training programs for crew and shore-based personnel**



GREENPORT
Alliances

Module 10 (Week 10)

COURSE NAME: Sustainable Maritime Operations and Green Ports

SECURITY PROCEDURES AND CRISIS MANAGEMENT IN A DIGITALIZED ENVIRONMENT



**Co-funded by
the European Union**

Disclaimer:

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. Project no. 101139879.