Introduction to Maritime Cybersecurity Risk Management

CSP001_S_M

PRESENTATION BY:
PINELOPI KYRANOUDI, CYBERSECURITY RESEARCHER AT TECHNICAL UNIVERSITY OF CRETE
NINETA POLEMI, PROFESSOR AT UNIVERSITY OF PIRAEUS

CyberSecPro

CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.

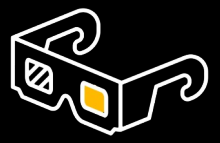
Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

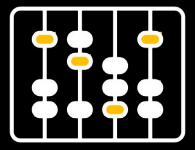
Goals: Who-What-Why you need to take this training

WHO



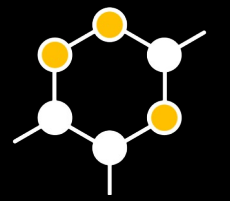
Professionals in maritime and port operations, cybersecurity, and management across IT, OT, and supply chain environments

WHAT



Seminar on cybersecurity risk management and certification in maritime systems, covering standards, controls, and supply chain security

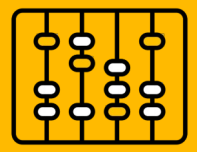
WHY



Enable participants to assess risk, support certification, and ensure secure and resilient maritime operations

CSP Training Logistic: When-Where-How

WHEN



Time schedule (to be posted in DCM platform)

WHERE

Physically, virtually, or both (to be posted in DCM platform)

HOW

Instructor-led sessions

Value Propositions

Benefits to Participants

- Level of Training Module: Advance
- Cybersecurity Professional Training
- Rooted with European Cybersecurity Skills Framework
- Cutting-edge insights from industry-academic experts
- Certificate of the completion
- Helps with skills development and career advancement

WHAT

Training Topics

- Introduction to Maritime Cybersecurity
- Understanding Maritime Cyber Risks
- Cybersecurity Standards and Best Practices
- Maritime Cybersecurity Certification

WHY

Learning Outcomes

Knowledge:

- Understanding of cybersecurity threats specific to the maritime sector.
- Familiarity with relevant cybersecurity frameworks, regulations, and standards governing maritime cybersecurity.
- Knowledge of cyber risks prevalent in maritime operations.
- Awareness of case studies and real-world examples of cybersecurity incidents in the maritime industry.
- Understanding of risk assessment methodologies and tools tailored to the maritime sector.
- Understanding of information security and maritime concepts.
- Understanding of best practices for securing maritime IT and OT systems.
- Knowledge of cybersecurity certification standards and schemes specific to the maritime industry.
- Familiarity with core concepts related to cybersecurity certification.
- Understanding of best practices for achieving and maintaining maritime cybersecurity certification.

WHO

Profiles of Trainers

- Pinelopi Kyranoudi has obtained her master's degree in Security of Information and Communication Systems from the University of the Aegean (Dept. of Information and Communication Systems Engineering). She served as Network and Information Security Officer at the European Union Agency for Cybersecurity (ENISA) contributing: to five publications in the areas of Cybersecurity in Maritime, e-Health, and National Cybersecurity Strategies; to the creation of web tools, and to the organization of EU Cybersecurity events. During her 10-year career she also worked in various positions and roles, such as Web and Application Developer, IT Security Engineer, Cybersecurity Researcher, and Lecturer in companies and organizations such as Express Publishing SA, Cosmote SA, Maggioli SpA, and Aegean College respectively, among others. She is currently conducting her Ph.D studies in the Cybersecurity field at the University of Piraeus (Dept. of Informatics). She holds a position of Cybersecurity Researcher at the Technical University of Crete (School of Electrical and Computer Engineering), contributing to EU research projects. Her research interests are in the field of Cyber-Physical Security, particularly in Maritime, OT/IoT, and Threat Intelligence.

- Nineta Polemi is a cybersecurity Professor in the University of Piraeus-UNIPI- (Cyber Security Lab, Dept. of Informatics) and CTO/ Co-Founder of Trustilio. She served (2017-2020) as Programme Manager and Policy Officer in the European Commission DG (CONNECT H1 Unit entitled 'Cybersecurity Technologies and Capabilities'). She has obtained her Ph.D. in Applied Mathematics (Coding Theory) from The City University of New York (Graduate Center). She held teaching and research positions in The City University of New York (Queens & Baruch Colleges), State University of New York (Farmingdale), Université Libre de Bruxelles (ULB)-Solvay Brussels School-. She has over 150 publications in security (e.g. port security, maritime security, maritime supply chain security) has organised numerous scientific and policy international cybersecurity scientific events. She has received many research grants (NATO, IEEE) and awards (NSA, MSI Army Research Office IEEE, CYNY, Hellenic Ministry of Maritime, Hellenic National Defense General) and has participated as Project and Technical Manager in more than 60 cybersecurity international, EU and national R&D and commercial projects. She serves as external expert/reviewer/consultant in ENISA, E.C. (DG CNECT, DG HOME), FORTH, Focal Point.

Training Outline

Topic-1: Introduction to Maritime Cybersecurity

Overview of cybersecurity threats in the maritime sector

Importance of maritime cybersecurity

Introduction to relevant cybersecurity frameworks and regulations (e.g., IMO Guidelines on Cyber Risk Management)

Topic-2: Understanding Maritime Cyber Risks

Identification of cyber risks in maritime operations

Case studies and real-world examples of cybersecurity incidents in the maritime industry

Risk assessment VS risk management

Training Outline

Topic-3: Cybersecurity Standards and Best Practices

Overview of cybersecurity standards applicable to the maritime industry (e.g., ISO 27001, NIST Cybersecurity Framework)

Overview of information security and maritime core concepts

Best practices for securing maritime IT and OT systems (e.g., ENISA Guidelines - Cyber Risk Management for Ports, CYSMET Risk Management Methodology)

Topic-4: Maritime Cybersecurity Certification

Cybersecurity certification standards and schemes applicable to the maritime industry (e.g., Common Criteria, EUCC)

Overview of cybersecurity certification core concepts

Best practices for maritime cybersecurity certification (e.g., CYRENE Risk & Conformity Assessment Methodology)

Background Knowledge and Prerequisites

Background knowledge:

Basic understanding of computers and networking

Familiarity with common internet security threats and vulnerabilities

Awareness of cybersecurity

Prerequisites:

None

Resources:
Reference Material

1. ISO/IEC 27001:2022, Information Security Management Systems — Requirements
2. ISO/IEC 27005:2018, Information Security Risk Management
3. ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation
4. ISO/IEC 18045, Common Evaluation Methodology for Information Technology Security Evaluation
5. NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments
6. NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations
7. NIST SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security
8. NIST, Cybersecurity Framework (CSF) 2.0
9. IEC 62443 Series, Security for Industrial Automation and Control Systems
10. International Maritime Organization (IMO), Guidelines on Maritime Cyber Risk Management
11. ENISA, Good Practices for Cybersecurity in the Maritime Sector
12. ENISA, Guidelines on Cyber Risk Management for Ports
13. ENISA, Transport Threat Landscape
14. European Union, EUCC (European Cybersecurity Certification Scheme)
15. CYRENE Project, Risk & Conformity Assessment Methodology for Maritime Supply Chains
16. Frontiers in Computer Science, Cybersecurity Risk Management Methodology for Supply Chain Systems (CYSMET), 2023

Course progress

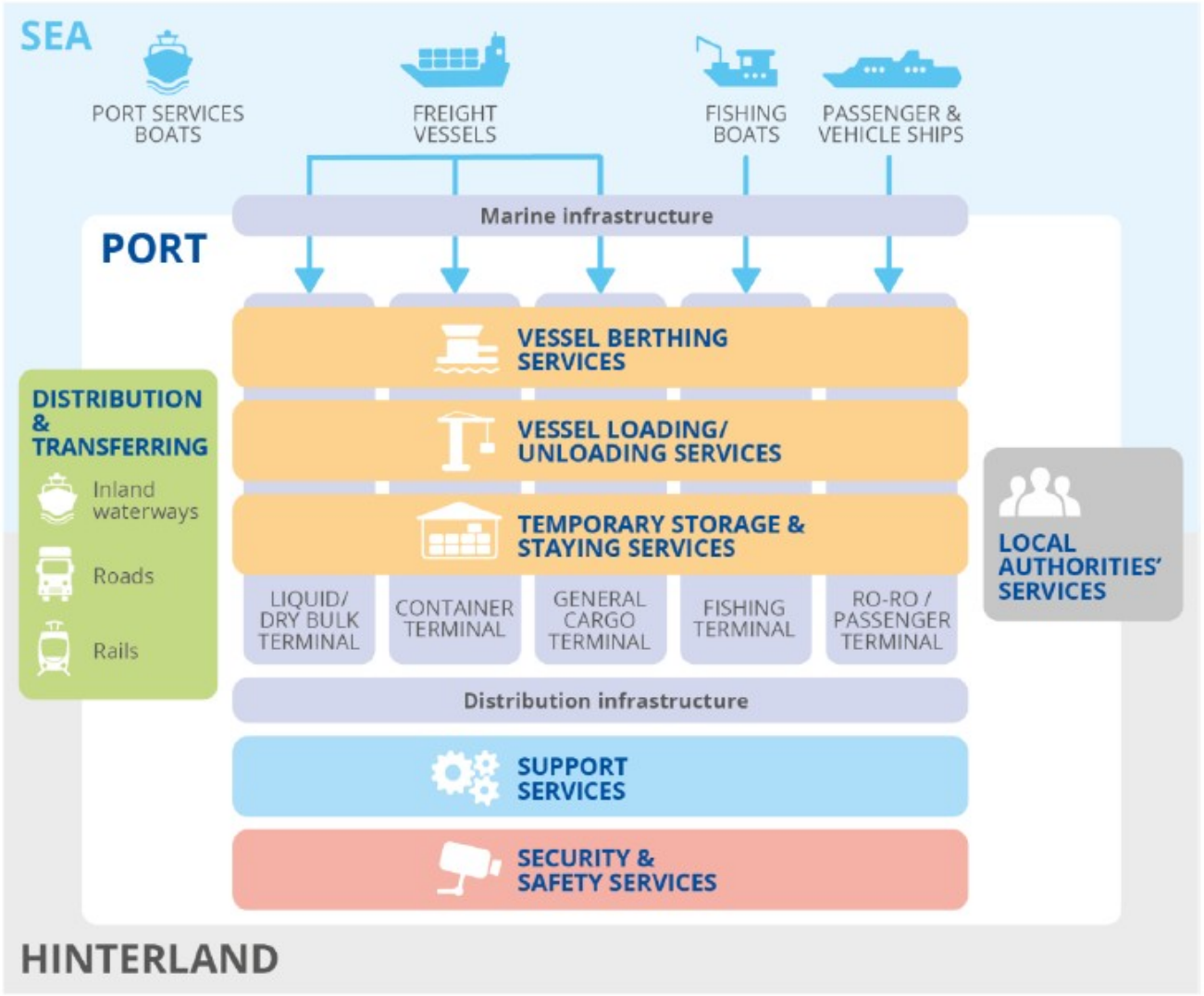
01. Introduction to Maritime Cybersecurity

02. Understanding Maritime Cyber Risks

03. Cybersecurity Standards and Best Practices

04. Maritime Cybersecurity Certification

Port Services and Infrastructure

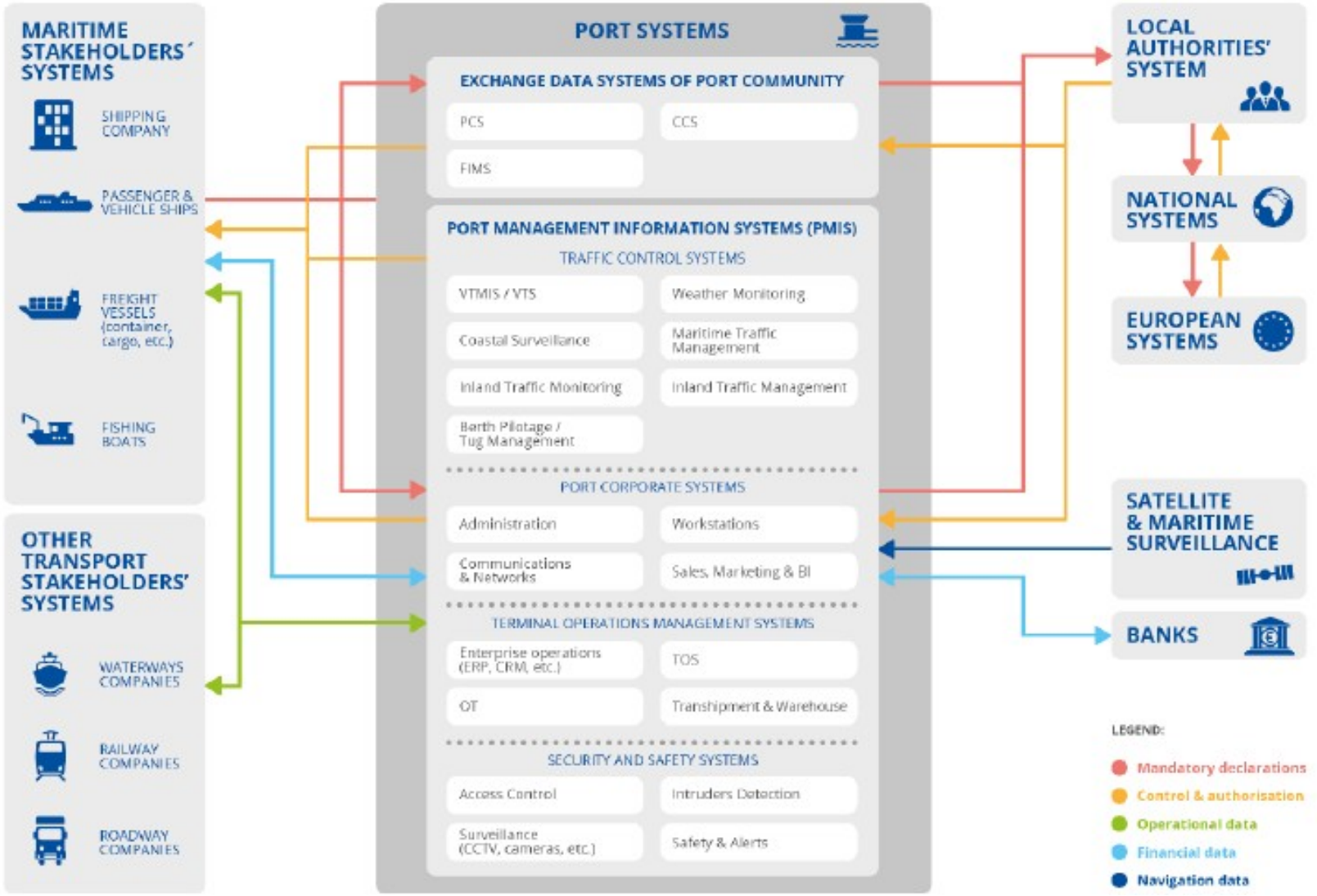


https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector?v2=1

What is Maritime Cybersecurity

- Protection of **interconnected maritime IT, OT and IoT systems** across ports, vessels and logistics networks
- **Focus on ensuring:**
  - **Safety** of vessels, crew and operations
  - **Integrity** of navigation and mission-critical systems
  - **Availability and Continuity** of port and supply chain operations
- **Addresses the unique challenges of:**
  - Highly **interconnected and distributed** environments
  - Integration of **IT, OT and IoT systems**
  - Exposure to both **cyber and physical risks**

High-level Reference Model of the Port Systems



https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector?v2=1

IT, OT and IoT Systems in Maritime Environments

- **IT systems:**
  - Booking platforms
  - ERP systems
  - Port community systems
- **OT systems:**
  - Navigation systems
  - Port equipment (cranes, control systems)
  - Vessel control systems
- **IoT / IIoT systems:**
  - Sensors (cargo, environment, equipment)
  - Smart devices and monitoring systems
  - Connected assets across ports and vessels
- **Increasing integration between IT, OT and IoT systems**
- **IoT significantly expands the attack surface**

What is a Threat?

Threat: A potential cause of an unwanted incident, which may result in harm to a system or organization.
[ISO/IEC 27000:2018]

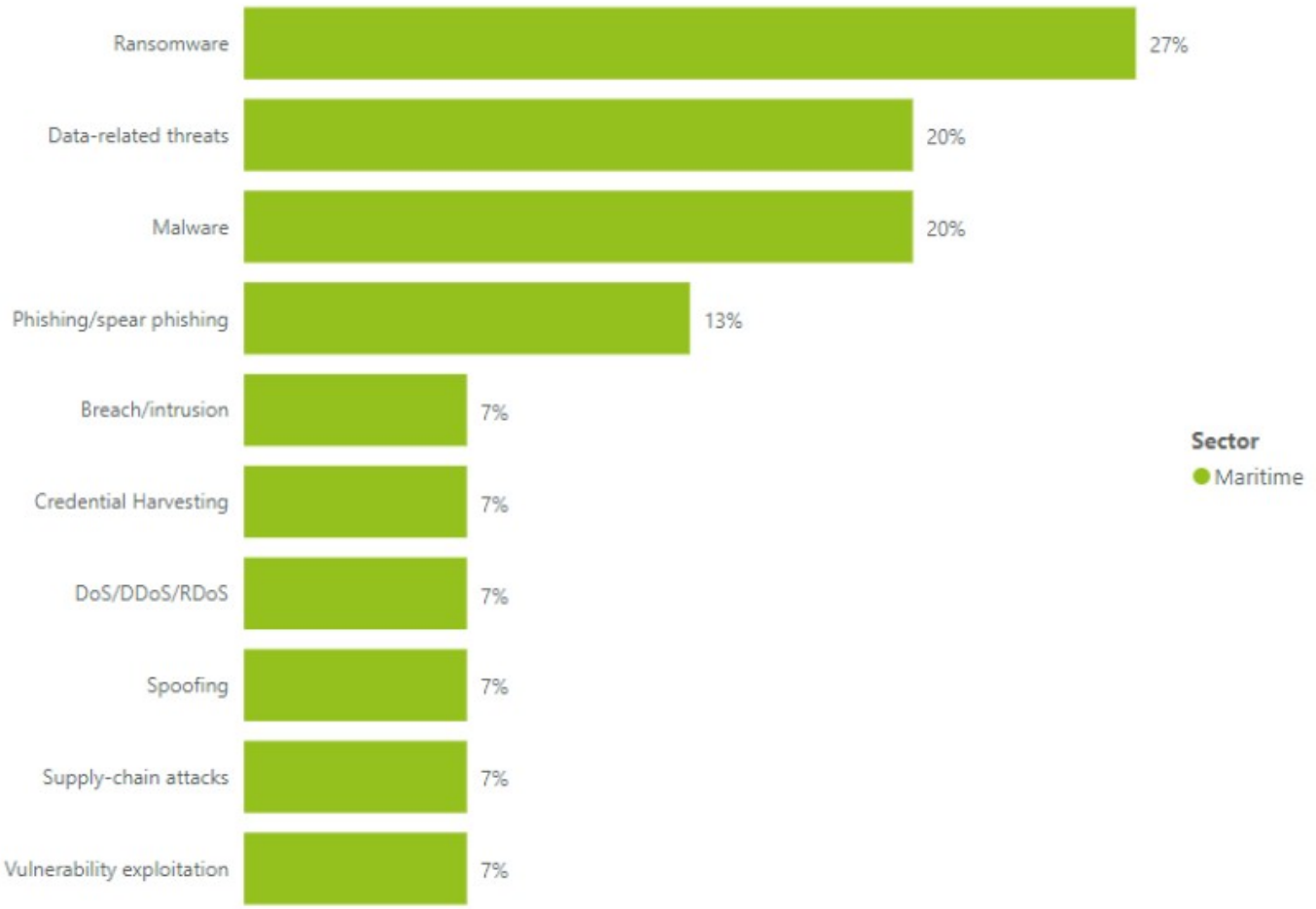
In this context, a threat is an external factor that could exploit a vulnerability in a system.
Threats can be human-driven (like attackers or insider threats), environmental (such as natural disasters), or technical (like malware or vulnerabilities in software).
The threat landscape in maritime cybersecurity would include risks from both intentional attacks (e.g., ransomware) and unintentional incidents (e.g., human errors).

https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape?v2=1

Types of Cyber Threats in Maritime

- **IT-related threats:**
  - Cyber attacks (ransomware, phishing, malware)
  - Web application attacks
  - Credential compromise
- **OT-related threats:**
  - Navigation attacks (e.g., GPS spoofing)
  - ICS / control system attacks
  - Physical-cyber attacks
- **IoT / IIoT-related threats:**
  - Compromised sensors and devices
  - Weak authentication mechanisms
  - Large-scale device exploitation
- **Human-related threats:**
  - Insider threats
  - Social engineering
  - Human error and misconfiguration
- **Cross-domain threats:**
  - Supply chain attacks
- **Threats can impact systems across vessels, ports and maritime infrastructure**

Maritime Prime Threats



https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape?v2=1

Why Maritime Systems are Highly Exposed to Cyber Threats

- **Complex ecosystem:** Ports, vessels, logistics and authorities
- **IT/OT convergence:** Interconnection of operational and business systems
- **High connectivity:** Satellite communications, remote access, third-party integration
- **Legacy systems:** Difficult to secure and maintain, often lack modern security controls
- **Safety-critical environment:** Cyber incidents can have direct physical impact

- **These factors significantly increase the attack surface and risk exposure**

Importance of Maritime Cybersecurity

https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

Importance of Maritime Cybersecurity

- **Protection of Critical Infrastructure:** Maritime operations are integral to global trade, transporting over 80% of goods worldwide. Cybersecurity ensures the protection of ports, shipping companies, and logistics networks from cyber threats.

- **Prevention of Disruptions:** Cyberattacks can lead to significant disruptions in shipping and port operations. For example, incidents like the Maersk cyberattack in 2017 resulted in major operational delays and losses exceeding $300 million.
-
- **Safeguarding Data Integrity:** Ensuring the integrity and confidentiality of sensitive data, such as navigational systems and cargo manifests, is crucial. Breaches can compromise safety and lead to financial losses.
-
- **Regulatory Compliance:** Increasing regulations, such as the International Maritime Organization's (IMO) guidelines, mandate robust cybersecurity measures to protect ships and ports, ensuring compliance can prevent legal repercussions.
-
- **Enhancing Safety:** Cybersecurity protects against threats that could endanger the safety of crew and vessels. Cyber incidents can manipulate navigation systems, posing risks to maritime safety.

- **Building Trust:** A strong cybersecurity posture fosters trust among stakeholders, including governments, customers, and partners. This trust is essential for the smooth operation of maritime supply chains.

Regulatory Drivers for Maritime Cybersecurity

- **Regulations:** Mandatory lLegal requirements that organizations must comply with
  - International Maritime Organization (IMO) requirements
  - EU regulations (e.g., GDPR, NIS2)
- **Standards:** Formalized requirements for implementing and managing security
  - ISO/IEC 27001
- **Frameworks:** Structured approaches for managing cybersecurity risk
  - NIST Cybersecurity Framework
- **Guidelines:** Recommended best practices and non-binding guidance
  - ENISA guidelines
  - IMO cyber risk management guidelines

- **Regulations require organizations to implement cybersecurity measures**
- **Standards and frameworks are used to achieve compliance and demonstrate security**

Course progress

01. Introduction to Maritime Cybersecurity

02. Understanding Maritime Cyber Risks

03. Cybersecurity Standards and Best Practices

04. Maritime Cybersecurity Certification

What is a Risk?

Risk: The effect of uncertainty on objectives (ISO 31000:2018; ISO/IEC 27000:2018). Risk is often characterized by reference to potential events and consequences or a combination of these (including changes in circumstances) and the associated "likelihood" of occurrence.
[ISO/IEC 27000:2018, ISO 31000:2018]

Vulnerability vs Threat vs Risk

- **Definitions:**
  - **Vulnerability:** a weakness that can be exploited
  - **Threat:** a potential cause of harm
  - **Risk:** the likelihood and impact of a threat exploiting a vulnerability

- **Example:**
  - **Vulnerability:** Poorly secured remote access to port systems
  - **Threat:** Unauthorized access attempt
  - **Risk:** Account compromise

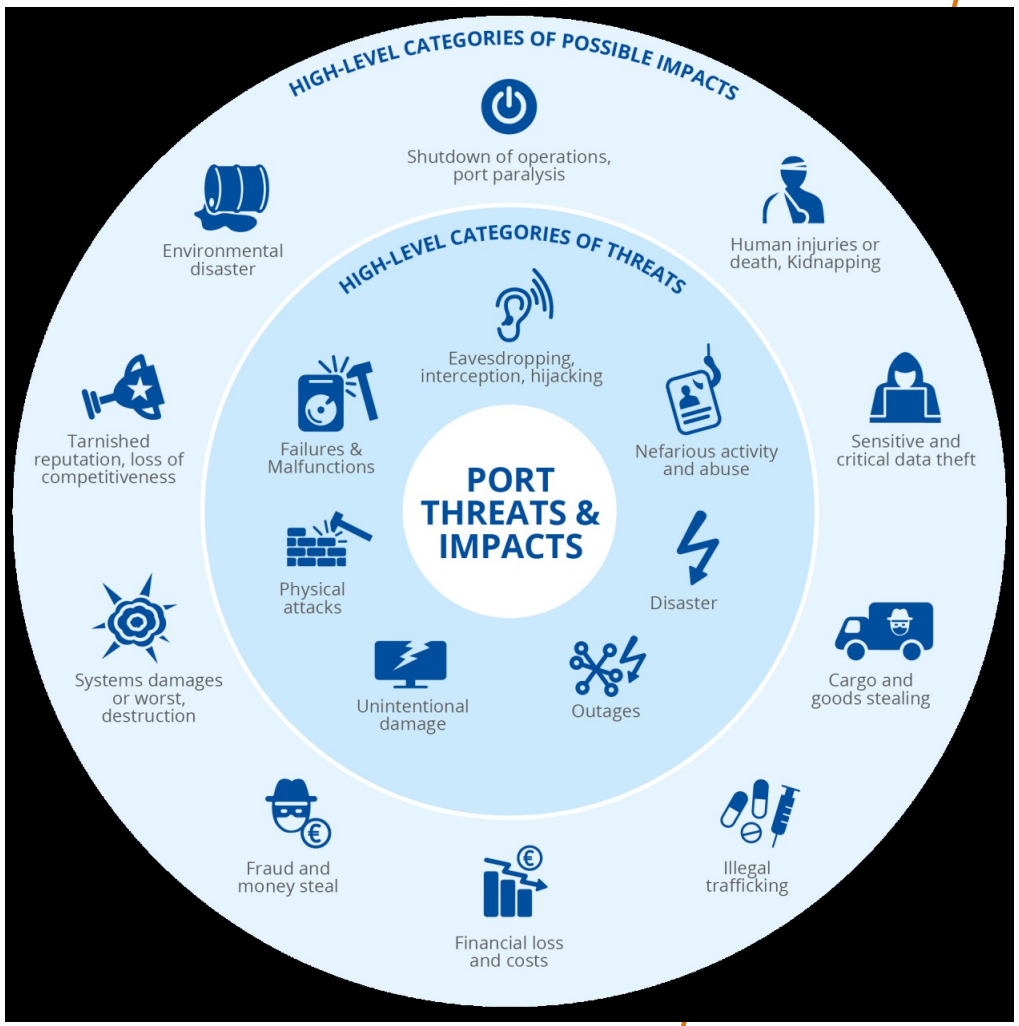
- **Risk exists only when there is a threat that can exploit a vulnerability**

Maritime Cyber Risk Scenarios and Their Impact

Risk Event Scenario	Potential Impact
Navigation system manipulation (e.g., GPS spoofing)	Incorrect positioning and potential safety impact on the vessel
Cargo data breach	Exposure of sensitive data and financial / reputational impact
Port operations disruption	Delays, congestion and impact on the supply chain
Ransomware on terminal systems	System unavailability, operational shutdown and financial loss

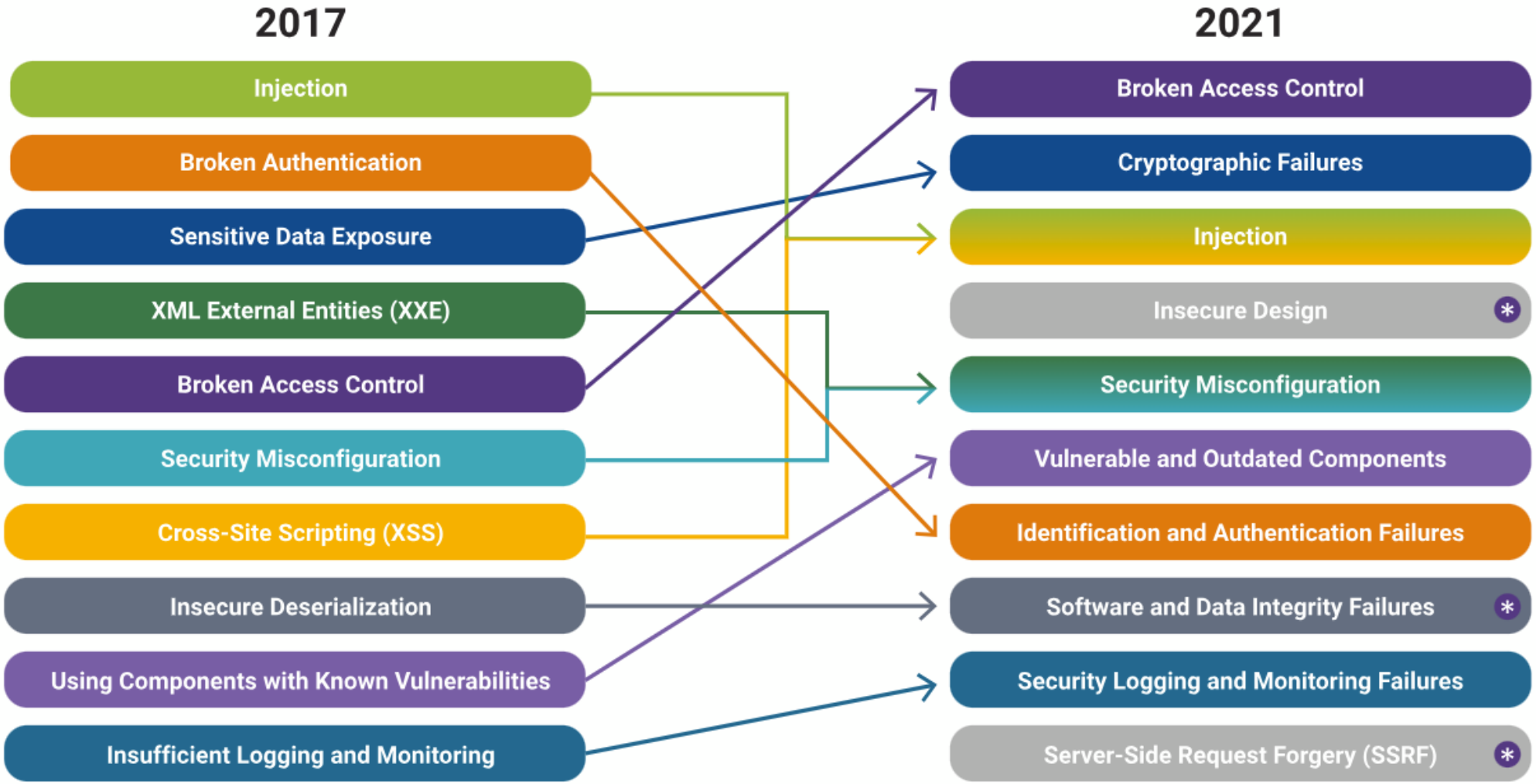
- **Cyber risks in maritime environments can impact safety, operations and business continuity**

Identification of Cyber Risks in Maritime Operations



https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports?v2=1

OWASP Most Critical Web Application Security Risks



OWASP Top 10:2024: https://www.owasptopten.org

Maritime Cybersecurity Incidents

Police warning after drug traffickers' cyber-attack

16 October 2013

Earlier this year drug traffickers hacked into the computer controlling shipping containers at the port of Antwerp

"In this case they hired hackers [who were] very high level, intelligent guys, doing a lot of software work," he adds.

He says the operation to hack the port companies took place in a number of phases, starting with malicious software being emailed to staff, allowing the organised crime group to access data remotely.

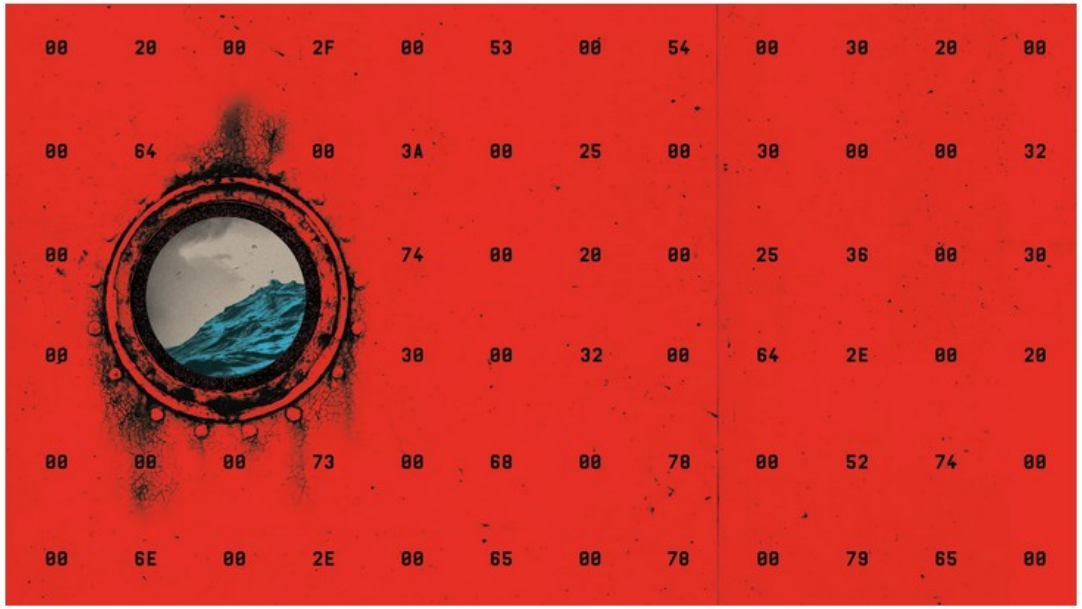
When the initial breach was discovered and a firewall installed to prevent further attacks, hackers broke into the premises and fitted key-logging devices onto computers.

This allowed them to gain wireless access to keystrokes typed by staff as well as screen grabs from their monitors.

Maritime Cybersecurity Incidents

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.



MIKE MCQUADE

Jensen looked up to ask if anyone else in his open-plan office of IT staffers had been so rudely interrupted. And as he craned his head, he watched every other computer screen around the room blink out in rapid succession.

"I saw a wave of screens turning black. Black, black, black. Black black black black black," he says. The PCs, Jensen and his neighbors quickly discovered, were irreversibly locked. Restarting only returned them to the same black screen.

[...] NotPetya's architects combined that digital skeleton key with an older invention known as Mimikatz, created as a proof of concept by French security researcher Benjamin Delpy in 2011. Delpy had originally released Mimikatz to demonstrate that Windows left users' passwords lingering in computers' memory. Once hackers gained initial access to a computer, Mimikatz could pull those passwords out of RAM and use them to hack into other machines accessible with the same credentials. On networks with multiuser computers, it could even allow an automated attack to hopscotch from one machine to the next.

Maritime Cybersecurity Incidents

Troubled waters: Cyber-attacks on San Diego and Barcelona's ports

03 Oct 2018

Our AI is actively defending ports across the world – such as Harwich Haven Authority and Belfast Harbour.

Last summer's wave of ransomware attacks compromised port terminals and disrupted global shipping. Since then, cyber security has quickly risen to the top of the agenda for the maritime sector. Earlier this year, another port was hit with ransomware, and then, last week, the ports of Barcelona and San Diego revealed that they had been the victims of further ransomware attacks.

The increasing convergence of IT and OT systems shows no signs of slowing, however. Hyper-connected 'smart' ports are bringing efficiency and precision while cutting costs. Yet, the intertwining of the physical and digital across ports remains a significant challenge for the cyber security teams tasked with their defense. Without rushing to conclusions, it is perhaps no surprise that the Port of Barcelona is in the process of a "Digital Port project," launched last year to promote the digitization of the port environment.

Human Factor in Maritime Cybersecurity

- In many maritime incidents, the **human is the weakest point** rather than the system
- **Phishing and social engineering** are common entry points for cyber attacks
- **Insider threats** include both malicious actions and unintentional mistakes by employees or contractors
- **Human error**, such as misconfiguration or weak credentials, introduces vulnerabilities in systems
- **Lack of awareness and cybersecurity training** increases exposure to attacks and reduces response capability
- Human actions can impact **IT, OT and IoT systems** across maritime environments

From IT to OT: How Attacks Escalate in Maritime

- **Step 1: Initial access (IT layer)**
  - Phishing email
  - Compromised credentials
  - Web application vulnerabilities
- **Step 2: Lateral movement (IT network)**
  - Access to internal systems
  - Privilege escalation
  - Movement across corporate network
- **Step 3: Pivot to OT / IoT systems**
  - Connection to operational systems
  - Weak network segmentation
  - Shared credentials or interfaces
- **Step 4: Operational impact**
  - Disruption of port operations
  - Navigation system interference
  - Equipment malfunction

- **Cyber incidents often start in IT but impact OT operations**

Incidents Analysis Using Risk Concepts

- What asset was affected?
- What vulnerability was exploited?
- What threat caused the incident?
- What was the impact on operations, safety or business?
- What controls could have prevented or mitigated the incident?

Risk Assessment vs Risk Management

Scope: Risk assessment focuses on identifying and evaluating risks, while risk management encompasses the entire process, including response and monitoring.

Process: Risk assessment is a subset of risk management; effective risk management cannot occur without a thorough risk assessment.

End Goals: The goal of risk assessment is to understand risks, while the goal of risk management is to manage those risks in a way that protects the organization and supports its objectives.

Risk Assessment Process

Phase	Step	Actions
Risk Assessment	1. Scope Definition	Define scope across ports, vessels and maritime systems (IT, OT, IoT)
	2. Asset & System Understanding	Identify critical assets, roles and dependencies
	3. Risk Identification	Threat identification, vulnerability discovery, exposure points
	4. Risk Analysis	Assess likelihood and impact on safety, operations and business
	5. Risk Evaluation	Prioritize risks based on defined criteria
Risk Treatment	6. Control Selection	Select appropriate security controls
	7. Treatment Strategy Definition	Define strategy (mitigate, accept, transfer, avoid)
	8. Control Implementation	Implement controls across IT, OT and IoT environments
Monitoring & Review	9. Monitoring & Review	Continuously monitor risks, evaluate controls and adjust

A high-level Example of Maritime Cyber Risk Management Methodology by ENISA

https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports?v2=1

Another Example of Risk Management Methodology

Main axes of risk analysis	CYSMET methodology
1. Perimeter/boundaries setting	Step 0: Scope of SCS risk assessment Step 1: Analysis of SCS *1.1 Scope and objectives of SCS* *1.2 Identification of SCS-BPs* *1.3 SCS modeling*
2. Threat analysis	Step 2: SCS threat analysis *2.1 Identification of cyber and/or physical individual threats linked to an SCS asset* *2.2 SCS threat assessment*
3. Vulnerability analysis	Step 3: SCS vulnerability and impact analysis *3.1 Determination of attacker profile* *3.2 Identification of confirmed individual vulnerabilities* *3.3 Identification of confirmed/zero-day vulnerabilities* *3.4 Creation of vulnerability chains in SCS* *3.5 Identification of attack methods and graphs* *3.6 Assessment of individual vulnerability severity level*
4. Impact analysis	
5. Risk assessment	Step 4: Risk assessment *4.1 Assessment of risk level of individual assets* *4.2 Vulnerability chain risk level assessment*
6. Risk mitigation strategy	Step 5: Risk mitigation—Selection of security controls

https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2023.1156726/full

Course progress

01. Introduction to Maritime Cybersecurity

02. Understanding Maritime Cyber Risks

03. Cybersecurity Standards and Best Practices

04. Maritime Cybersecurity Certification

Why Cybersecurity Standards & Frameworks Matter

- **Cybersecurity cannot rely on ad-hoc measures or isolated solutions**
- Organizations need a **structured approach** to manage risks consistently
- Standards ensure **consistent protection across IT, OT and IoT systems**, define clear and measurable **security controls**, and enable **alignment with regulatory and operational requirements**
- They allow organizations to make **risk-based decisions**, demonstrate security through **audits**, and prepare for **certification and compliance**

Key Maritime Cybersecurity Standards & Frameworks

- **ISO/IEC 27001:2022:** International standard for establishing and maintaining an information security management system (ISMS), ensuring confidentiality, integrity and availability of information through a systematic approach.
- **NIST Cybersecurity Framework:** Risk-based framework that helps organizations identify, protect, detect, respond to and recover from cybersecurity threats.
- **GDPR (General Data Protection Regulation):** EU regulation defining requirements for the protection of personal data, applicable also to maritime organizations handling EU citizens' data.
- **IMO Cyber Risk Management:** Guidelines for integrating cybersecurity into maritime operations and safety management systems to protect shipping and port activities.
- **ENISA (European Union Agency for Cybersecurity) Guidance**: Cybersecurity recommendations and best practices for maritime and port environments, supporting risk-based protection and resilience of critical infrastructure.

Challenges in Applying Cybersecurity Standards in Maritime

- **Legacy OT systems are difficult to update or secure**, as they were not designed with cybersecurity in mind and often cannot support modern controls
- **Systems often cannot be taken offline**, as continuous operation is required, limiting the ability to apply patches or perform maintenance
- **Security measures must not interfere with safety and operations**, requiring careful balance between protection and operational continuity
- **Multiple stakeholders** (ports, operators, vendors) share systems and responsibilities, making consistent implementation of controls more complex

Core Security Controls in Maritime Systems

- **Access control and identity management** ensures only authorized users and systems can access critical maritime systems
- **Network segmentation** limits the spread of attacks between corporate and operational environments
- **Monitoring and incident detection** enables early detection of suspicious activity across systems
- **System hardening and patch management** reduces vulnerabilities, while considering operational constraints
- **Backup and recovery** ensures systems and data can be restored after disruption or cyber incidents

Course progress

01. Introduction to Maritime Cybersecurity

02. Understanding Maritime Cyber Risks

03. Cybersecurity Standards and Best Practices

04. Maritime Cybersecurity Certification

What is Cybersecurity Certification

- **A formal process to evaluate and verify** the security of systems or products
- **Based on certification schemes and evaluation standards** (e.g., Common Criteria, EUCC)
- Performed by **independent and accredited evaluation bodies**
- Requires **defined security requirements, testing and assurance levels**
- **Results in a certified level of trust** in the security of the system or product

Certification vs Compliance

Aspect	Compliance	Certification
Definition	Meeting regulatory or legal requirements	Formal evaluation against defined security criteria
Assessment	Self-declared or internal	Independent third-party assessment
Scope	Laws, regulations, policies	Certification standards and schemes (e.g., Common Criteria, EUCC)
Outcome	Demonstrates adherence	Provides verified assurance and trust

Why Certification Matters in Maritime

- **Regulatory and compliance expectations:** Certification helps organizations align with regulatory requirements
- **Business and contractual requirements:** Often required by partners, clients and supply chain stakeholders
- **Risk reduction across interconnected systems:** Provides assurance in complex maritime ecosystems
- **Trust and credibility:** Builds confidence between ports, operators and third parties
- **Competitive advantage:** Demonstrates maturity and differentiates organizations in the market

Common Cybersecurity Certification Standards & Schemes

- **Common Criteria (ISO/IEC 15408)** – Certification of IT products and systems based on security evaluation
- **Common Evaluation Methodology (ISO/IEC 18045)** – Defines the methodology for evaluating products under Common Criteria
- **EUCC (European Cybersecurity Certification Scheme)** – EU framework for certifying ICT products and services

Certification Process Overview

- **Define the Target of Evaluation (TOE)** (system or product within scope)
- **Select an applicable Protection Profile (PP)** or define requirements for the evaluation
- **Define the Security Target (ST)** describing how the TOE meets the required security objectives
- **Perform independent security evaluation and testing** based on established evaluation methodology
- **Assessment conducted** by accredited evaluation laboratories and certification bodies
- **Certification issued with a defined assurance level** indicating the level of confidence in the security of the system
- **Maintain certification** through updates, surveillance and re-evaluation

Challenges in Maritime Certification

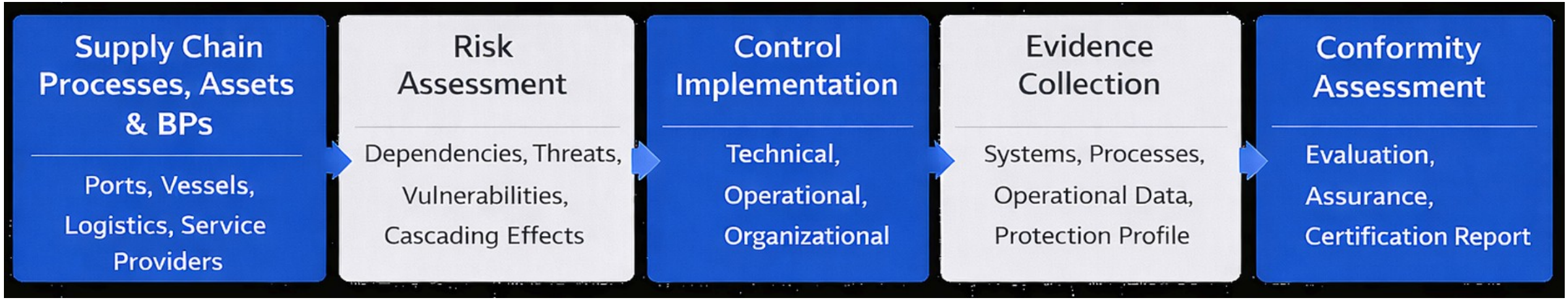
- **Defining certification scope across vessels and ports:** Systems span ships, port infrastructure and logistics networks, making the Target of Evaluation difficult to isolate
- **Evaluating systems in operational environments:** Limited ability to perform testing on live systems due to continuous operation and safety constraints
- **Heterogeneous and legacy maritime systems:** Diverse technologies and older equipment complicate alignment with modern evaluation requirements
- **Maritime supply chain dependencies:** Certification must consider interconnected systems across operators, ports, vendors and logistics providers

Risk & Conformity Assessment in Maritime Supply Chains

- **Certification extends** beyond individual systems **to interconnected maritime supply chain services** (ports, vessels, logistics, service providers)
- Assessment is based on:
  - **Risk analysis across interconnected business processes, assets and Business Partners (BPs)**, including dependencies and cascading effects
  - **Implementation of controls** across organizational and technical boundaries
  - **Collection of evidence** from multiple stakeholders (systems, processes, operations)
- **CYRENE Risk & Conformity Assessment Methodology** introduces a Maritime supply chain-oriented approach that supports both implementers and assessors
- Emphasis on both:
  - **Risk-driven** security at ecosystem level
  - **Evidence-based** conformity and continuous evaluation

CYRENE Risk & Conformity Assessment Methodology

Abstract depiction of CYRENE Methodology



Thank you

Please send all questions to:
pkyranoudi@tuc.gr
dpolemi@unipi.gr

CyberSecPro