EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA REPORT ON GOOD PRACTICES FOR PORT CYBERSECURITY

Dr. Athanasios Drougkas
Expert in Network and Information Security
ENISA – The EU Agency for Cybersecurity

ENISA Maritime Cybersecurity Workshop
26 | 11 | 2019

AGENDA

ENISA's work in maritime cybersecurity

- Overview of ENISA's activities
- Previous ENISA work in maritime
- TRANSSEC

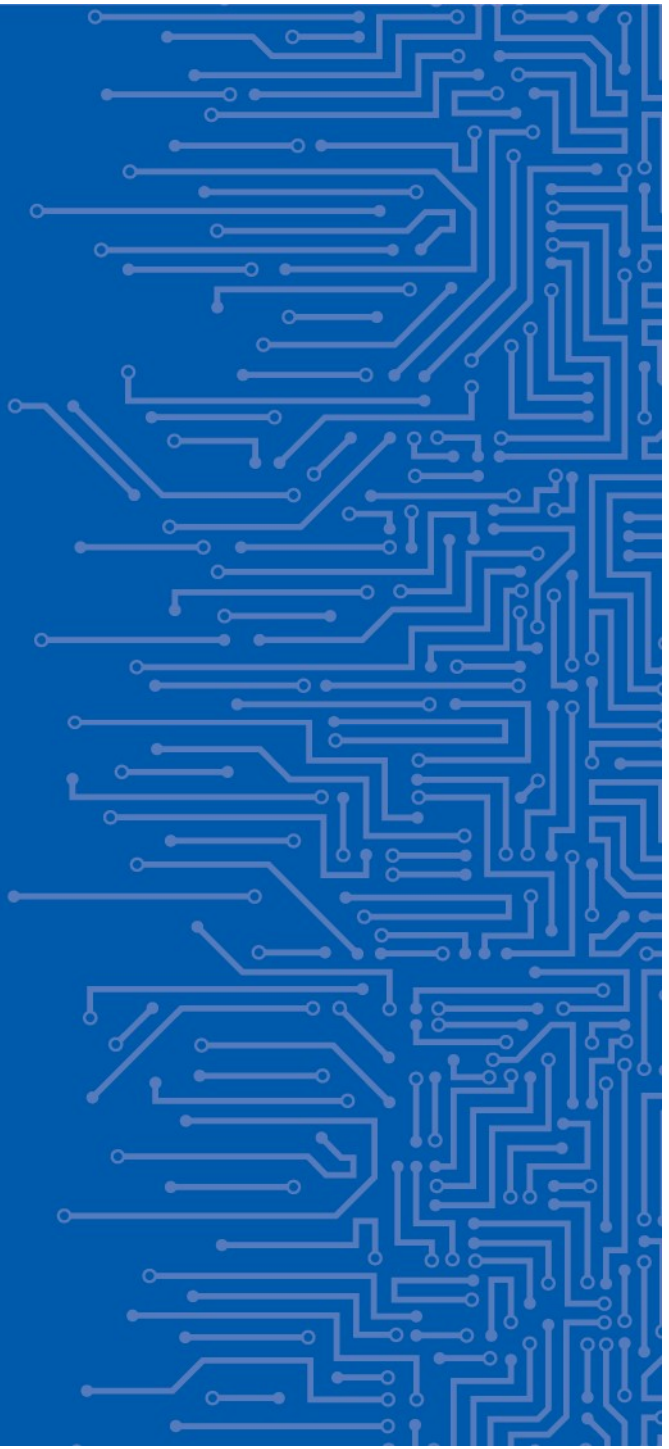
ENISA's 2019 report on port cybersecurity

- Presentation of main findings
- Discussion on conclusions / recommendations

Open discussion on future ENISA activities in maritime

- ENISA's 2020 report
- Brainstorming / other suggestions

ENISA'S WORK IN MARITIME CYBERSECURITY



POSITIONING ENISA'S ACTIVITIES

1

RECOMMENDATIONS ON CYBER SECURITY AND INDEPENDENT ADVICE

2

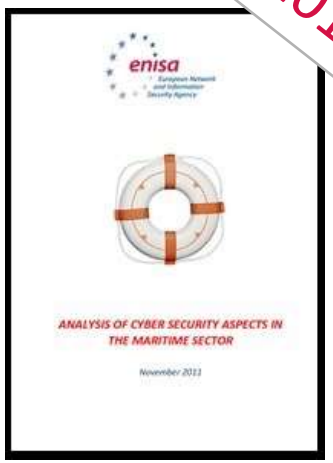
SUPPORT MS & EC IN POLICY IMPLEMENTATION AND HARMONISATION ACROSS EU

3

'HANDS-ON' WORK, COLLABORATING WITH OPERATIONAL TEAMS THROUGHOUT EUROPE

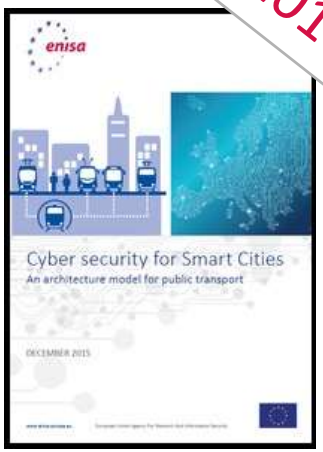
RELEVANT ENISA REPORTS

2011



2016

2016



2016

2017

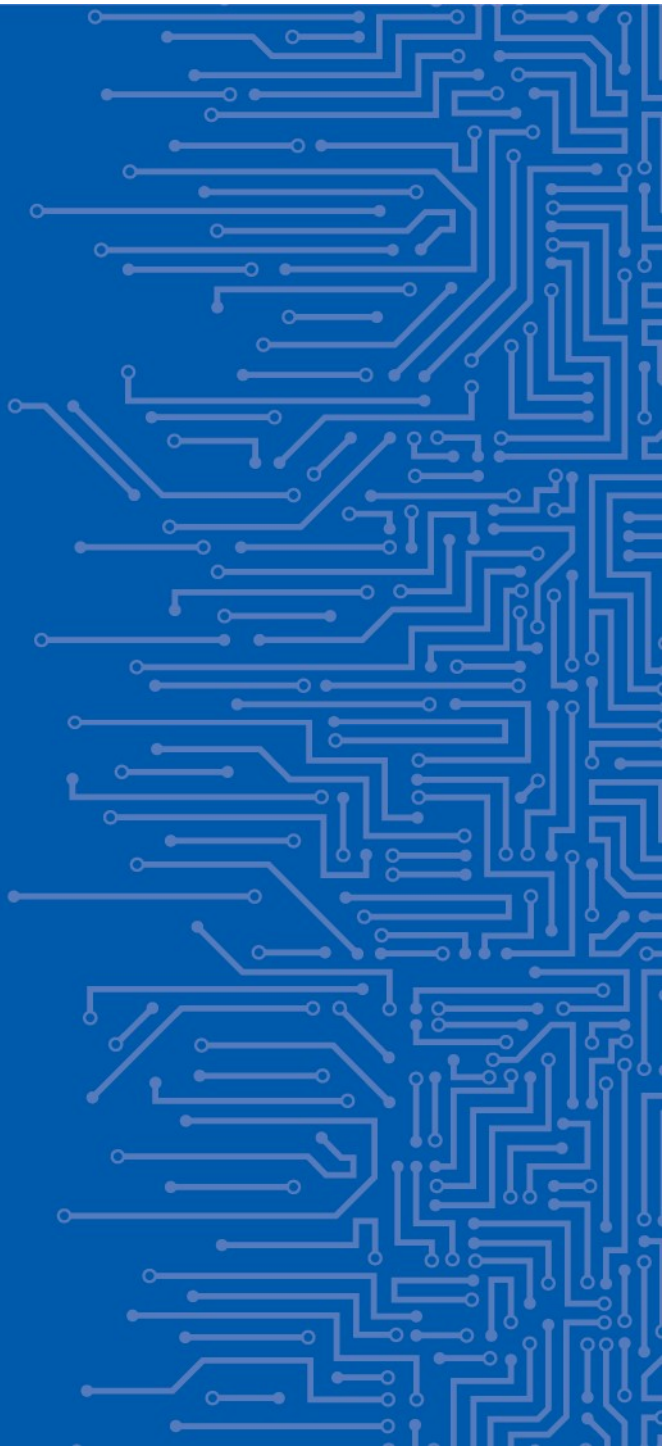
2017

TRANSSEC – MARITIME WORK STREAM

WORKSHOP AGENDA AND OBJECTIVES

26 NOVEMBER, 2019	EVENT	SPEAKERS / PANELLISTS
	WELCOME SESSION	
08.30 - 09.00	Registration & Welcome Coffee	
09.00 - 09.05	Welcome & Opening	**Dr. Athanasios Drougkas**, NIS Expert, ENISA
09.05 - 09.20	Welcome speech	**Maja Markovčić Kostelac**, Executive Director, EMSA
09.20 - 09.40	Cybersecurity in the Maritime Sector: Implementation of the EU regulatory framework and EC initiatives	**Dr. Nineta Polemi**, Programme Manager- E.U. Policies, DG CONNECT, European Commission
09.40 - 10.00	Implications of addressing the needs of cybersecurity in the conduct of the European Commission's maritime security inspections	**Christian Dupont,** Senior expert – Inspections de Sûreté Maritime, DG MOVE, European Commission
10.00 - 10.15	Cyber threats: adapting and updating your Port facility security assessment	**Luca Gargano**, Project Officer for Maritime Security & **Ruben Panes**, Project Officer for Port State Control & Environment, EMSA
10.15 - 10.35	Situational awareness: known cybersecurity incidents targeting ports	**Chronis Kapalidis**, Europe Representative, Hudson Cyber
	ENISA'S 2019 REPORT ON GOOD PRACTICES FOR PORT CYBERSECURITY	
10.35 - 11.15	Presentation of study findings and open discussion	**ENISA**
11.15 - 11.30	**Coffee break**	
11.30 - 13.00	ENISA's work in maritime cybersecurity • Discussion on 2019 ENISA report (continued) • Discussion on ENISA's future activities	**ENISA**, **Audience**
13.00 - 14.00	**Lunch offered**	
	INFORMATION SHARING IN THE MARITIME SECTOR	
14.00 - 14.20	ENISA's recommendations for ISACs	**Dr. Athanasios Drougkas**, NIS Expert, ENISA
14.20 - 14.40	Good practices from European Rail ISAC	**Olivier de Visscher**, Co-Chair of the European Rail ISAC
14.40 - 15.00	Good practices from Port of Rotterdam ISAC	**Ward Veltman**, Cyber Security & Risk Officer, Program manager FERM, Port of Rotterdam & **Elserike Looije,** Senior advisor maritime cybersecurity, National Cyber Security Center The Netherlands
15:00 - 15:20	How to create the PPP and ISAC in cybersecurity – the roadmap	**Magdalena Wrzosek,** Head of Strategic Analysis and Emerging Technologies Team, NASK PL
15:20 – 15:30	**Coffee break**	
15.30 - 16.15	**Discussion panel: Good practices for ISACs** Previous speakers & audience (Moderator ENISA)	
16.15 - 16.30	Conclusions, open discussion & wrap up	**ENISA, Audience**

ENISA 2019 REPORT: GOOD PRACTICES FOR PORT CYBERSECURITY



PORTS ARE UNDER ATTACK!

CNBC

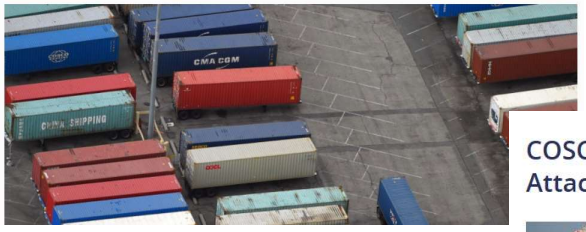
MENU MARKETS BUSINESS NEWS INVESTING TECH POLITICS CNBC TV

ENTERPRISE

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GUIDE

Shipping company Maersk says June cyberattack could cost it up to $300 million

Long Beach Port terminal hit by ransomware attack



Michael Murray, SVP and GM, BlackRidge Technology
August 27, 2019

Share

COSCO Shipping Lines Falls Victim to Cyber Attack

COSCO Shipping Lines confirmed that it has been hit by a cyber attack impacting its internet connection within its offices in America.

Police warning after drug traffickers' cyber-attack

By Tom Bateman
Reporter, Today programme

16 October 2013 Share

The head of Europe's crime fighting agency has warned of the growing risk of organised crime groups using cyber-attacks to allow them to traffic drugs.

The director of Europol, Rob Wainwright, says the internet is being used to facilitate the international drug trafficking business.

His comments follow a cyber-attack on the Belgian port of Antwerp.

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

Drug traffickers recruited hackers to breach IT systems that controlled the

Worried about cyber pirates hijacking autonomous ships? Focus on port cybersecurity first

One cyber attack can cost major APAC ports $110B

In an "extreme" scenario, a single software virus infecting 15 ports across five Asian markets including Singapore, Japan, and China, can result in losses totalling $110 billion, estimates a new study, which notes 92% of such costs remain uninsured.

Port of San Diego suffers cyber-attack, second port in a week after Barcelona

Cyber-attacks have now been reported at three ports in the last two months

Port of Barcelona Suffers Cyberattack

By Ionut Ilascu September 21, 2018 05:15 PM 0

ENISA 2019 REPORT: PORT CYBERSECURITY

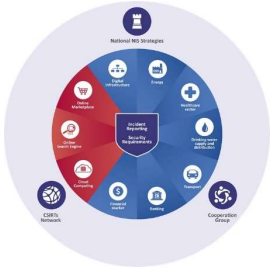
- **Good practices for cybersecurity in the maritime sector (port security)**
  - **Target audience**: Port CISOs/CIOs
  - **Scope**: Entire port ecosystem, IT/OT
  - **Interviews** with 14 stakeholders of the port ecosystem from 11 MS
  - **Objectives**: build a baseline of good practices to ensure cybersecurity of port systems and services
  - **Contents**:
    - High-level reference model
    - Asset Taxonomy
    - Threat taxonomy
    - Attack Scenarios
    - Security Measures

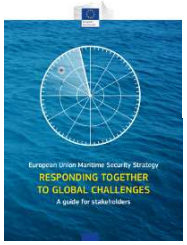
EU AND INTERNATIONAL POLICY CONTEXT

International

IMO
INTERNATIONAL MARITIME ORGANIZATION

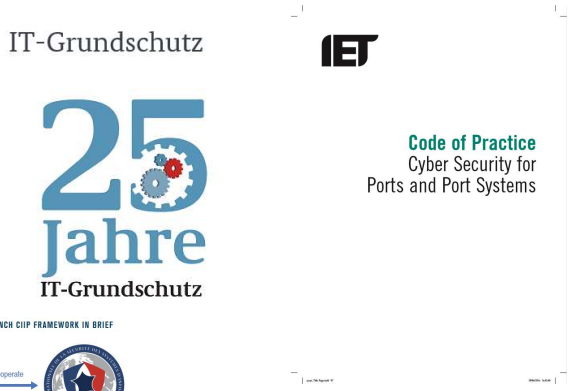
EU-level

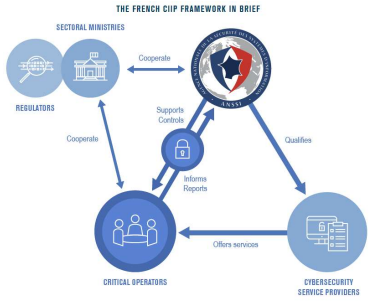




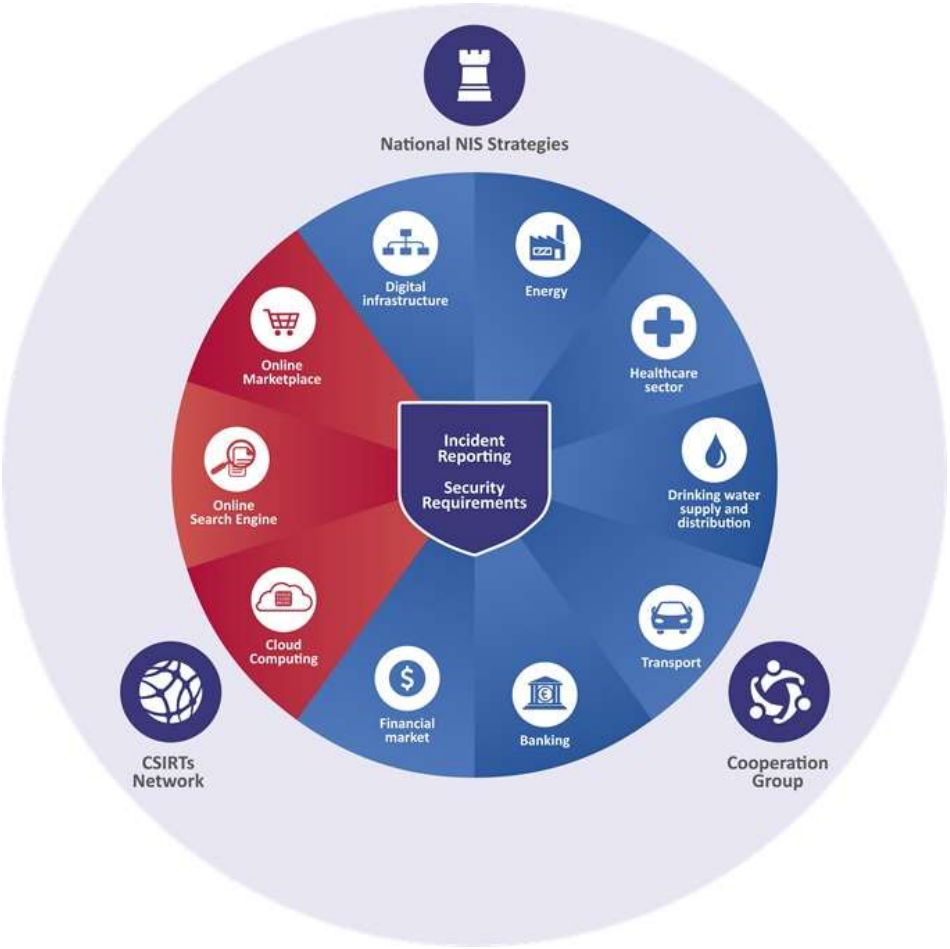
EMSA
SafeSeaNet

National





THE NETWORK AND INFORMATION SECURITY DIRECTIVE



IDENTIFICATION OF OES IN THE WATER TRANSPORT SECTOR

MS shall define the criteria for the identification of OES and identify the OES among the following:

- **Inland, sea and coastal passenger and freight water transport companies** (Annex I to Regulation (EC) No 725/2004)
- **Managing bodies of ports** (point (1) of Article 3 of Directive 2005/65/EC), **including their port facilities** (point (11) of Article 2 of Regulation (EC) No 725/2004), **and entities operating works and equipment contained within ports**.
- **Operators of vessel traffic services** (point (o) of Article 3 of Directive 2002/59/EC)

CYBERSECURITY ACT

EUROPEAN
COMMISSION

Brussels, 13.9.2017
COM(2017) 477 final

2017/0225 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

(Text with EEA relevance)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

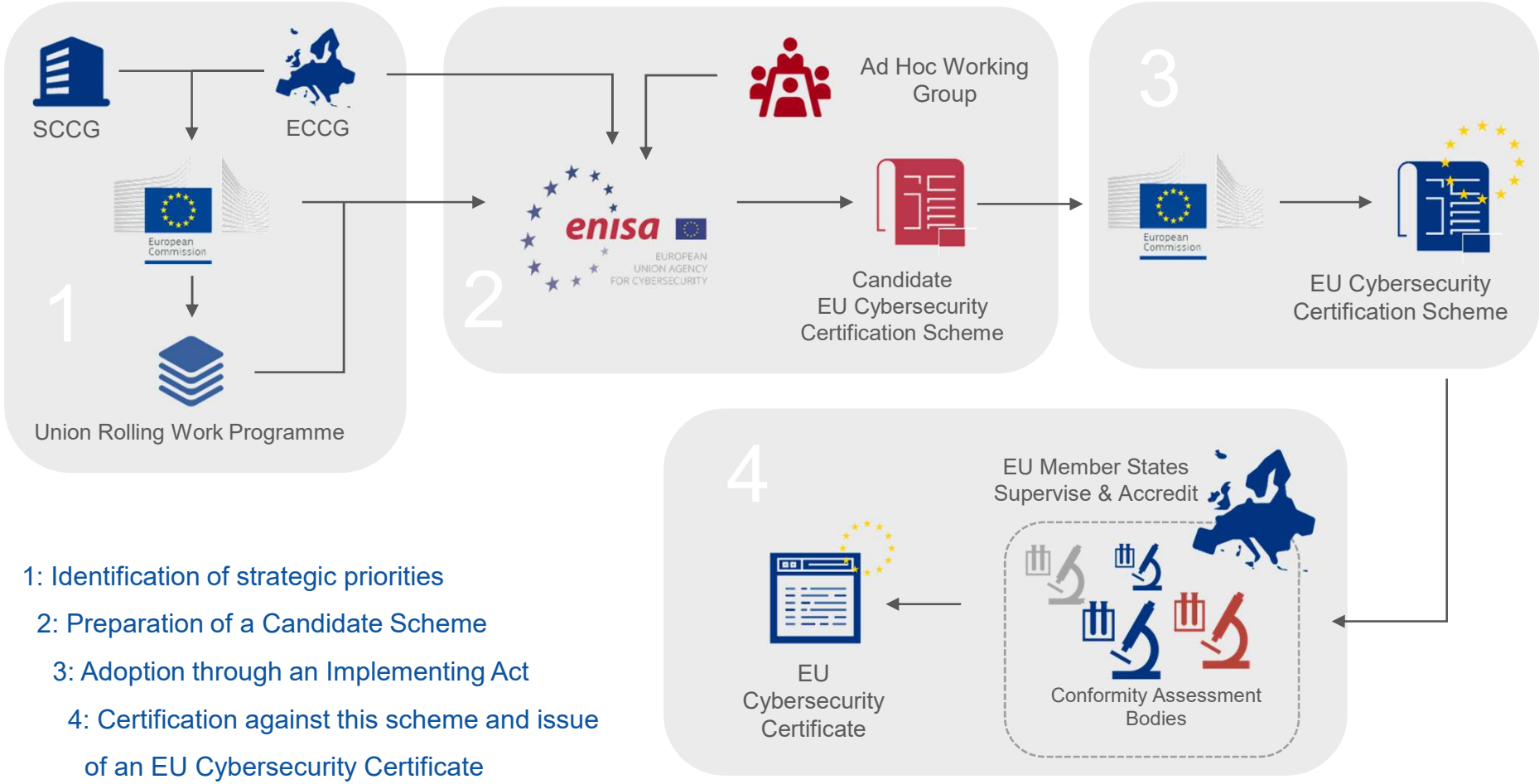
ENISA Reform

- An **EU Agency for Cybersecurity**
- Stronger Mandate
- Permanent Status
- Adequate Resources

EU Cybersecurity Certification Framework

- One framework, many schemes
- Certificates valid across all MS
- Roles for MS and ENISA
- Voluntary and risk-based approach; any need for mandatory schemes to be identified

THE EU CYBERSECURITY CERTIFICATION FRAMEWORK



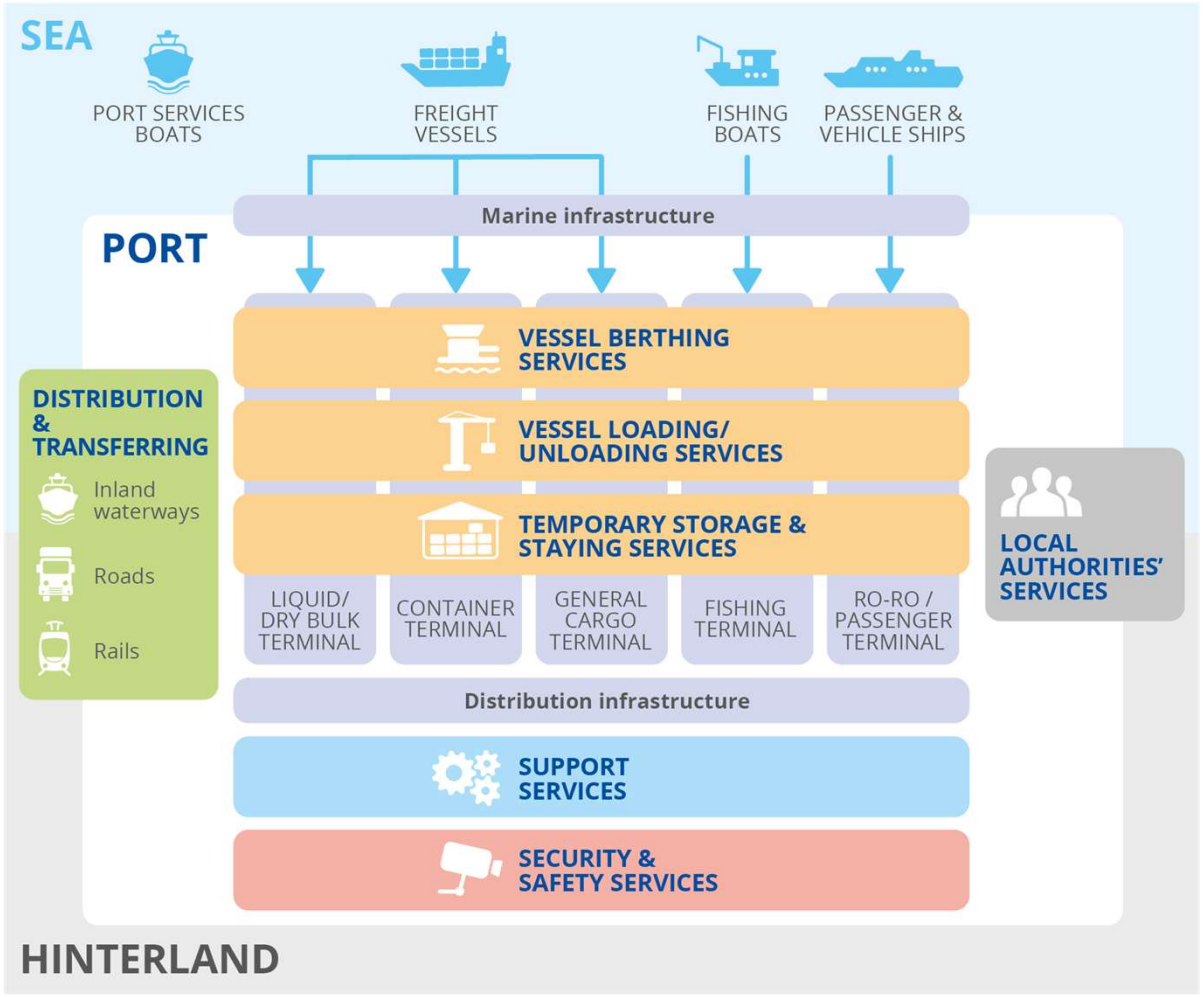
1: Identification of strategic priorities

2: Preparation of a Candidate Scheme

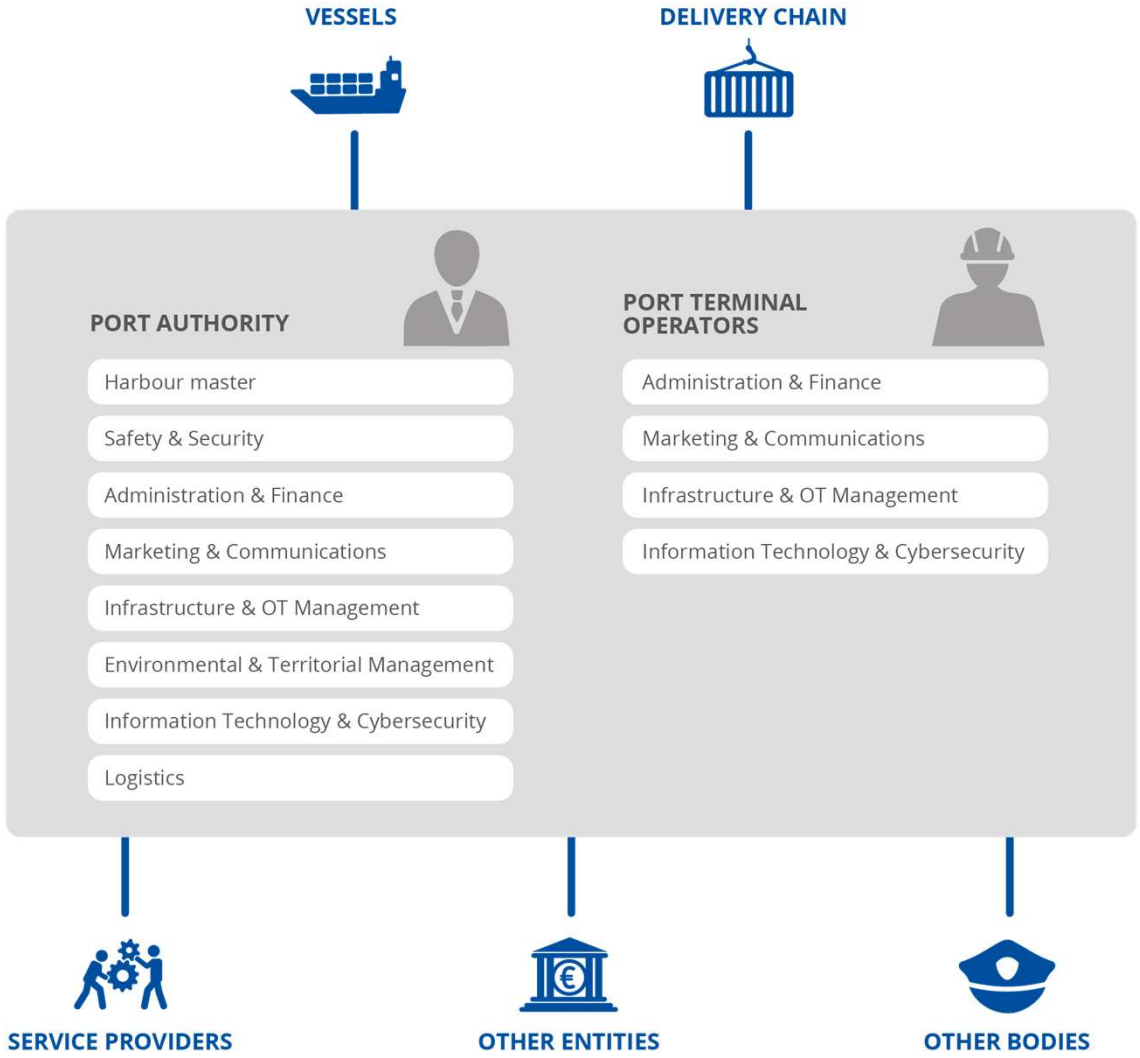
3: Adoption through an Implementing Act

4: Certification against this scheme and issue of an EU Cybersecurity Certificate

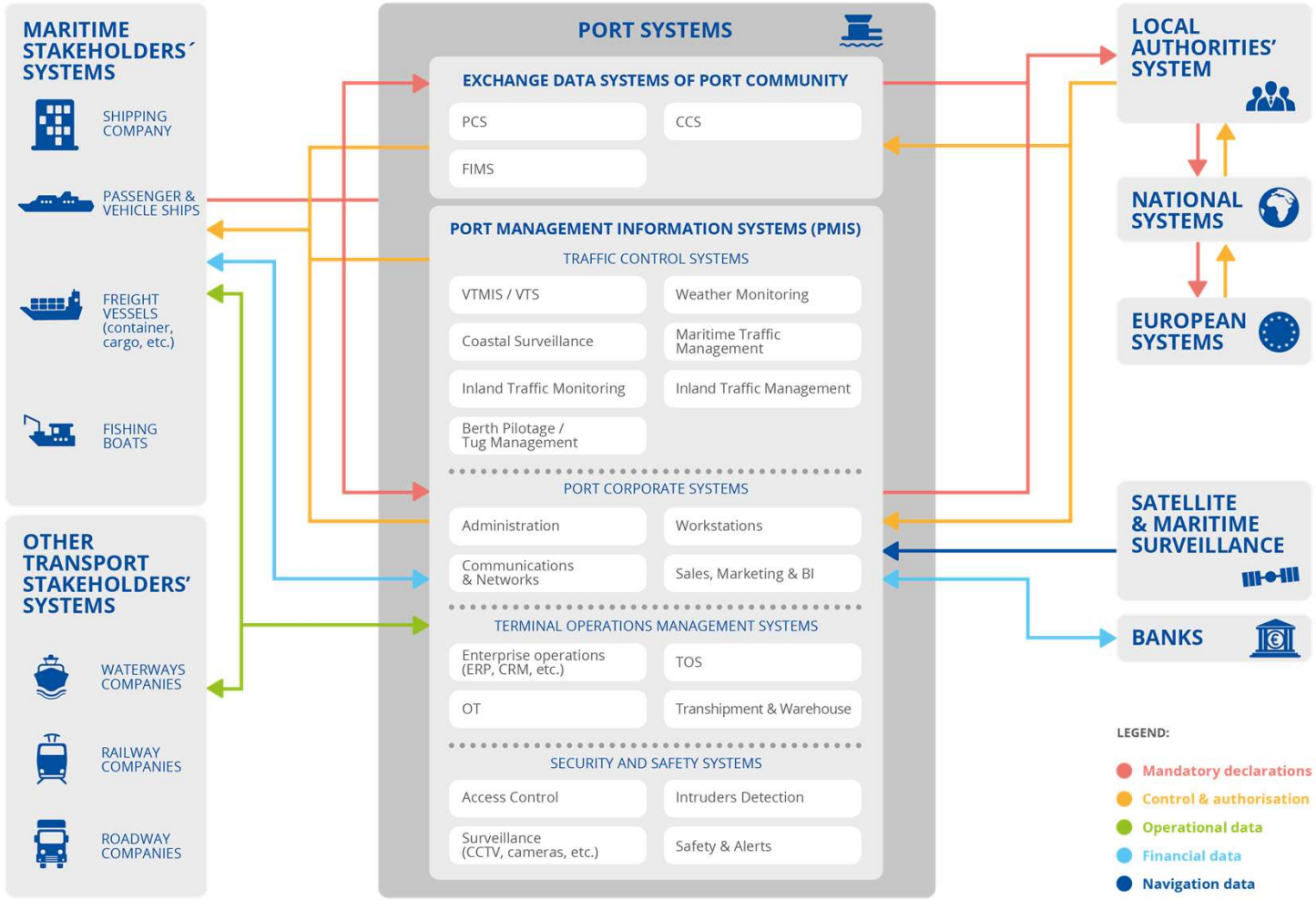
PORT SERVICES AND INFRASTRUCTURE



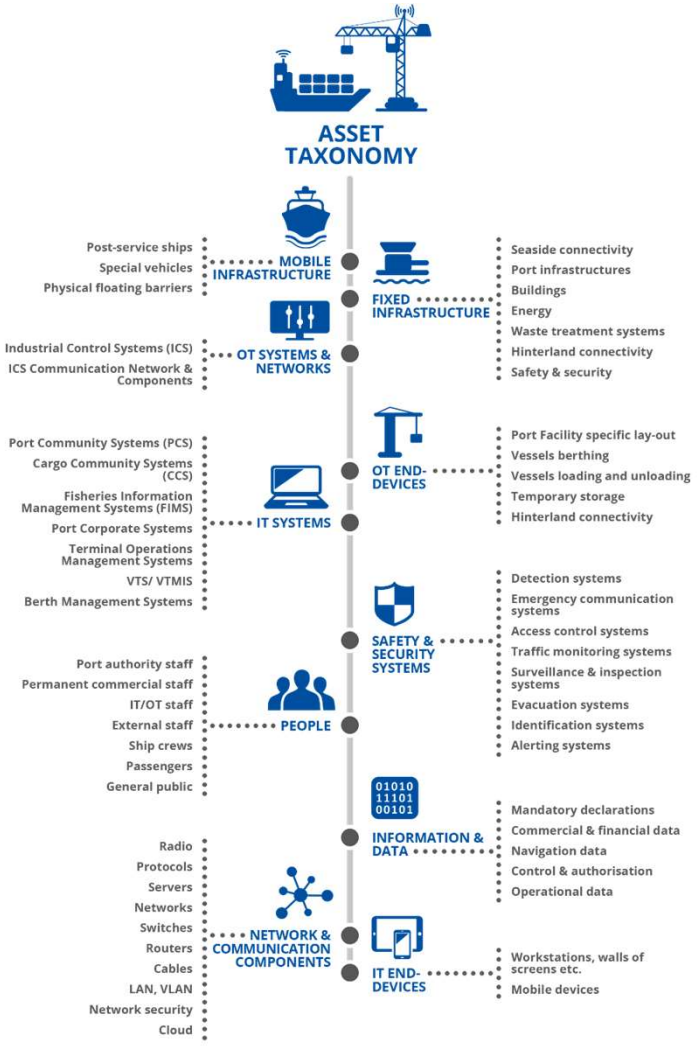
OVERVIEW OF PORT STAKEHOLDERS



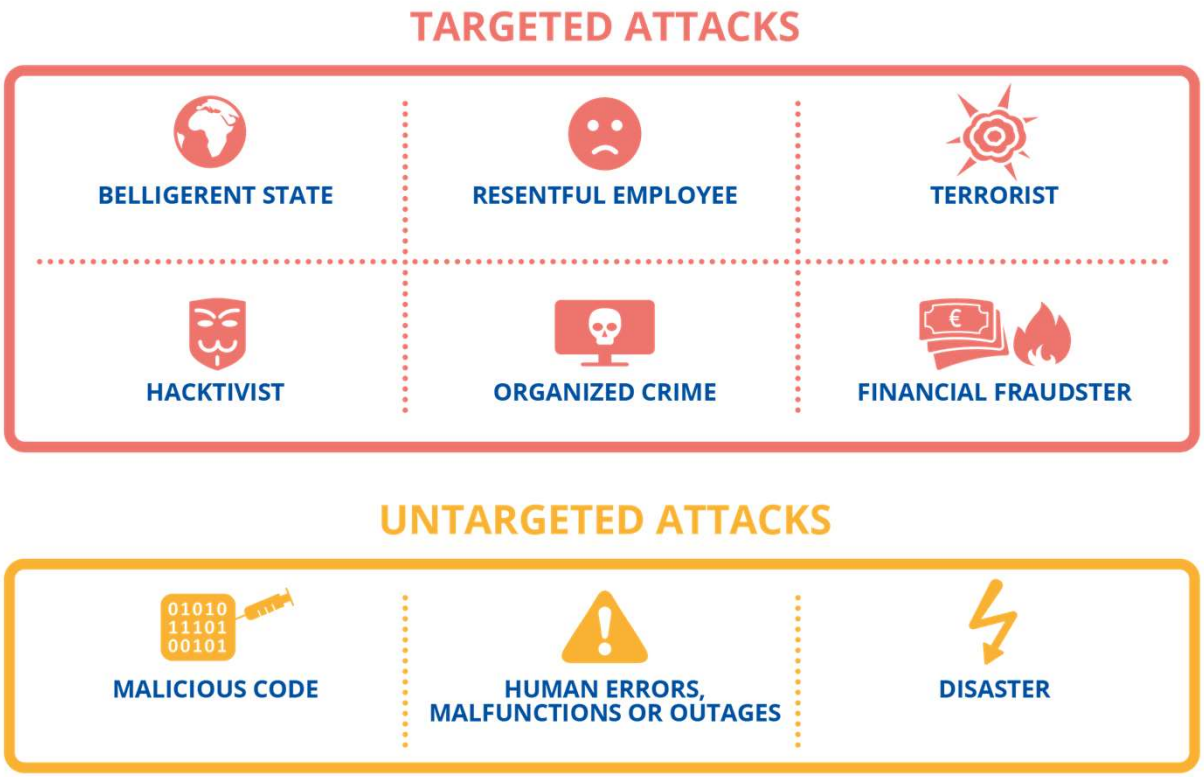
PORT SYSTEMS REFERENCE MODEL



PORT ASSET TAXONOMY



PORT CYBERSECURITY THREATS – MAIN SOURCES OF ATTACKS



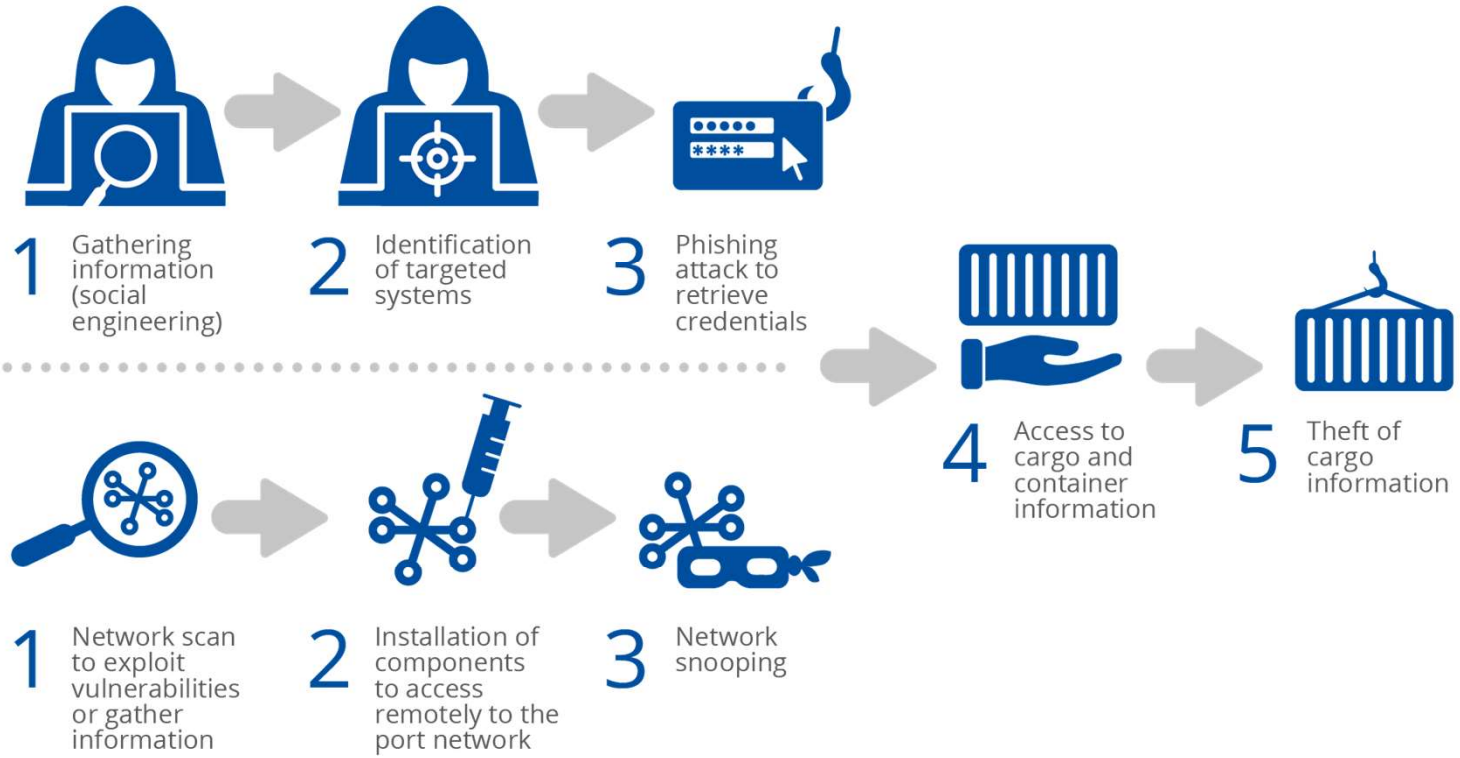
PORT CYBERSECURITY THREATS – POSSIBLE IMPACTS FOR PORTS

PORT CYBERSECURITY THREATS – THREAT TAXONOMY

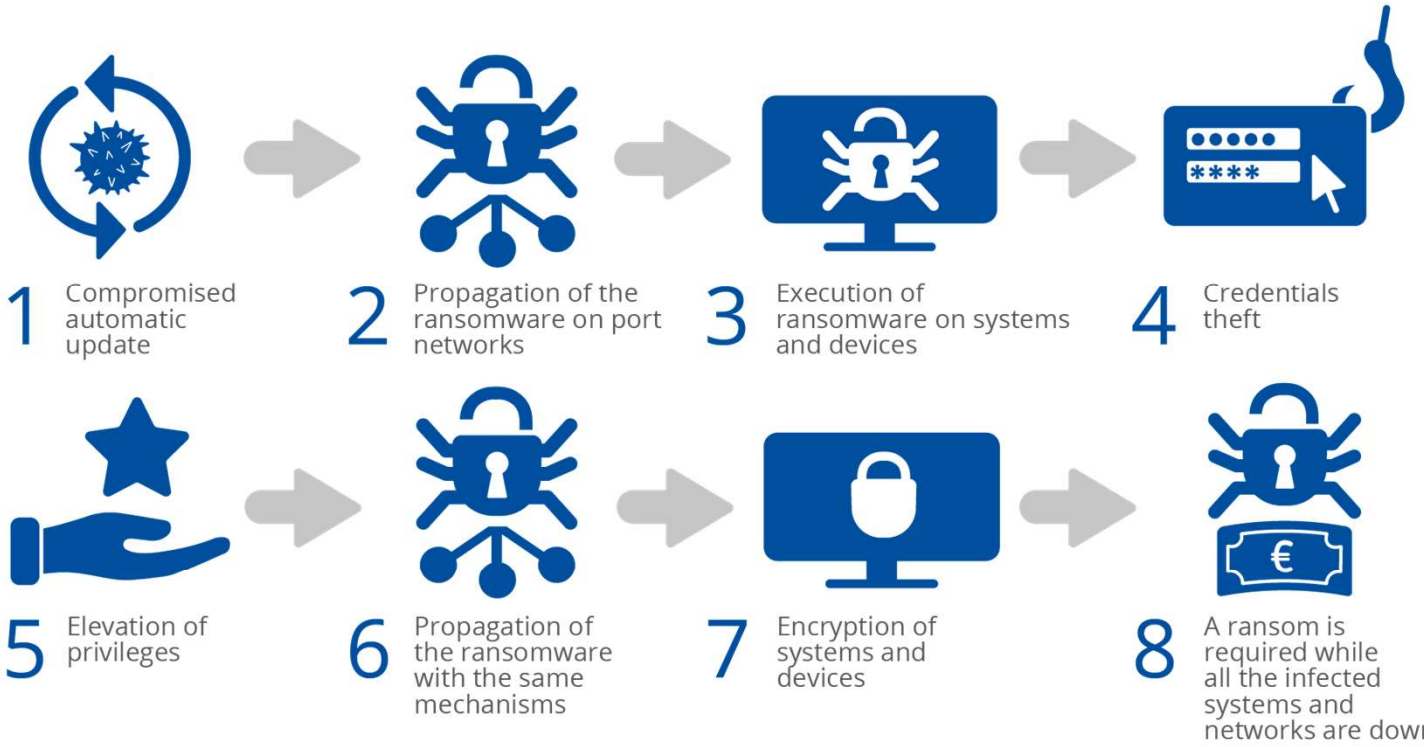
CYBERSECURITY CHALLENGES

- **Lack of digital culture** in the port ecosystem
- Lack of **awareness and training**
- **Lack of time and budget** allocated to cybersecurity
- Lack of **human resources** and qualified people
- **Complexity** of port ecosystem / diversity of stakeholders in operations
- Balance between business **efficiency and cybersecurity**
- **Legacy systems** and practices
- **Lack of regulatory requirements** regarding cybersecurity
- Difficulty to stay **up to date with the latest threats**
- **Technical complexity** of port IT and OT systems
- **IT and OT convergence** and interconnection
- **Supply chain** challenges
- Strong **interdependencies**
- **New cyber risks** from the digital transformation of ports

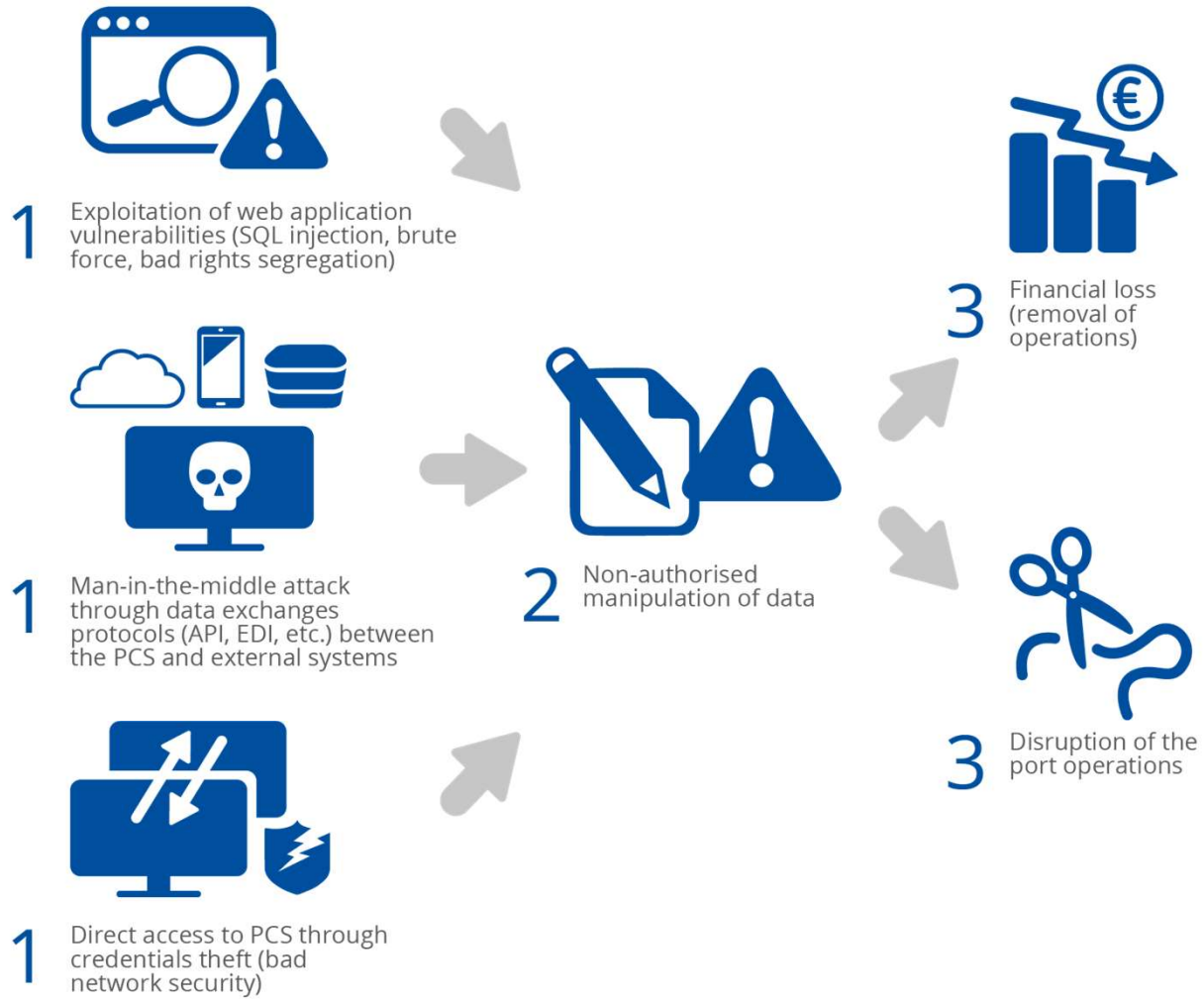
ATTACK SCENARIO: MANIPULATION OR THEFT OF CARGO / CONTAINER



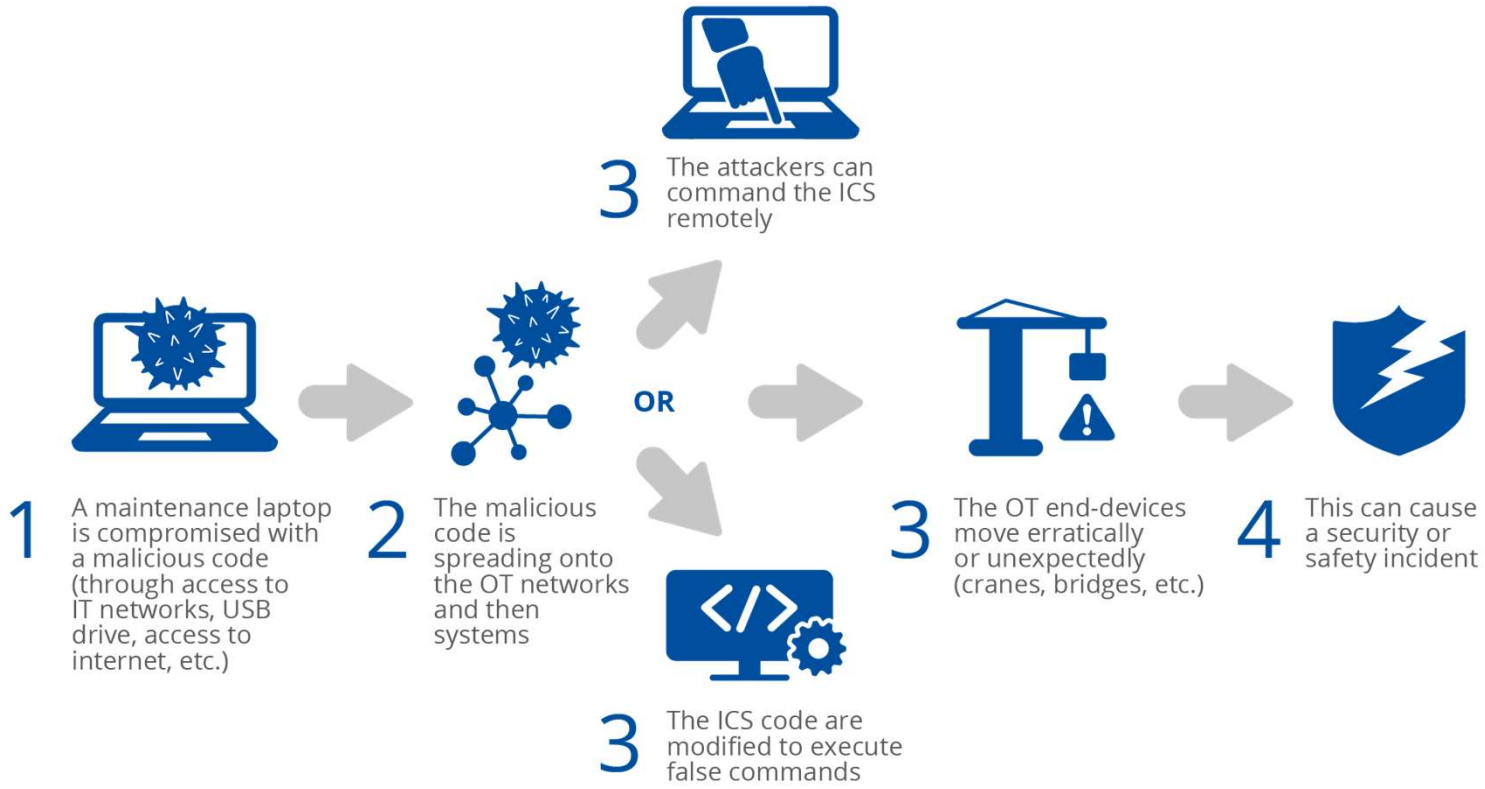
ATTACK SCENARIO: RANSOMWARE



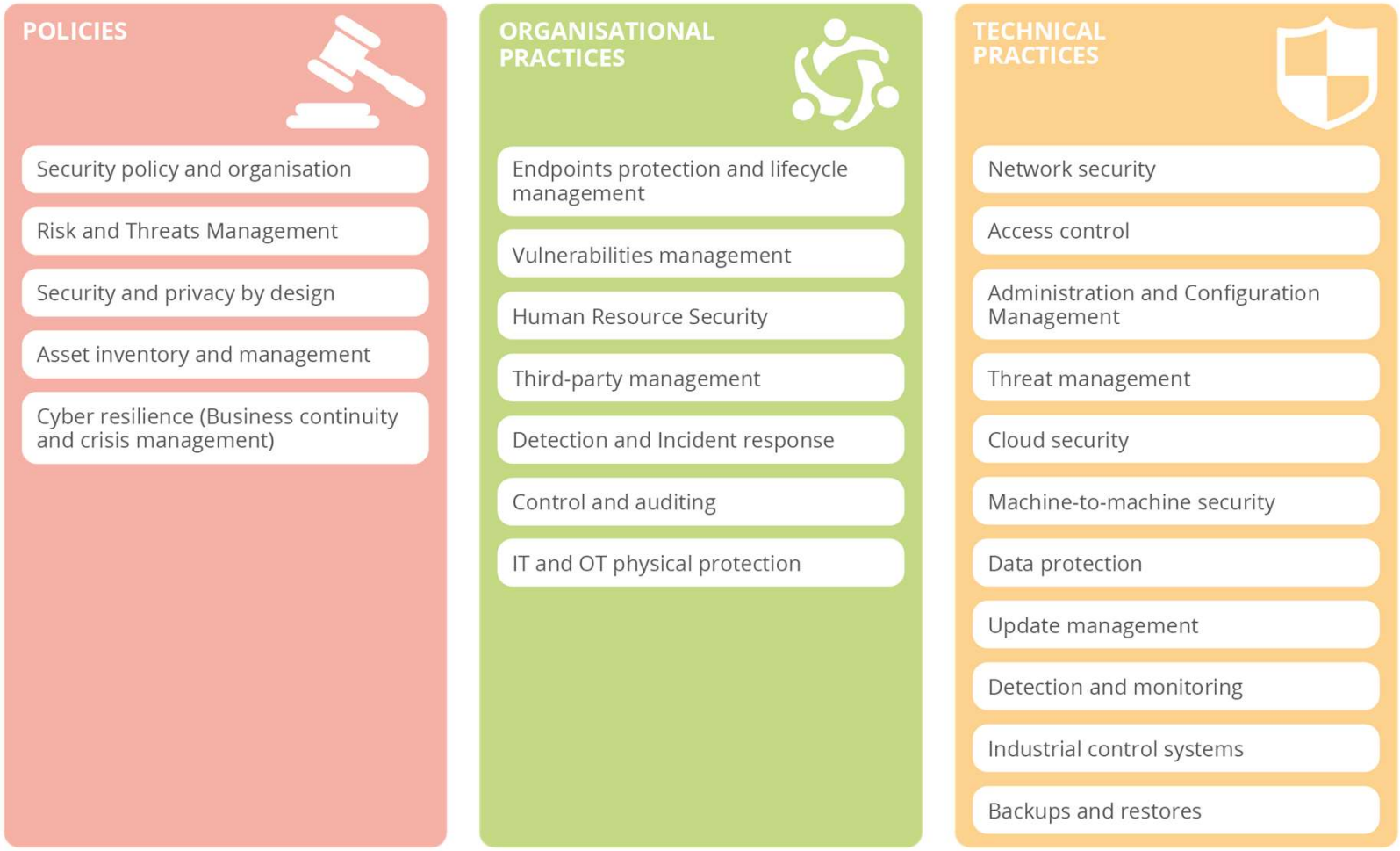
ATTACK SCENARIO: COMPROMISE OF PCS



ATTACK SCENARIO: COMPROMISE OF OT



SECURITY MEASURES



SECURITY MEASURES - POLICIES

Security policy and organisation
PS-01: ISSP
PS-02: Security governance
PS-03: Share ISSP with all stakeholders
PS-04: Review ISSP annually

Risks and threats management
PS-05: Risk-based approach
PS-06: Conduct and update risk analysis
PS-07: Security indicators
PS-08: Threat intelligence process

Security and privacy by design
PS-09: Project methodology including security
PS-10: Privacy and compliance
PS-11: Data classification

Asset inventory and management
PS-12: Asset inventory and management
PS-13: Policy for authorized devices/software
PS-14: Asset monitoring

Cyber resilience
PS-15: Define objectives and strategic guidelines (BCP and DRP).
PS-16: Business continuity parameters (RTO, RPO, MTO etc.)
PS-17: Crisis management
PS-18: Training/exercises for recovery procedures

SECURITY MEASURES – ORGANISATIONAL PRACTICES

Endpoints protection and lifecycle management

OP-01: Endpoint protection strategy
OP-02: Device and software whitelisting
OP-03: Change management
OP-04: Return and disposal of end-devices

Vulnerabilities management

OP-05: Vulnerability management process
OP-06: Intelligence processes for cybersecurity
OP-07: Collaboration of OT and IT departments

Human resources security

OP-08: Professional references of key personnel
OP-09: Cybersecurity training
OP-10: Security awareness raising program

Third party management

OP-11: Third-party access control
OP-12: Partnership with third parties

Detection and incident response

OP-13: Define categories of incidents
OP-14: Policy and procedures for incident detection and response
OP-15: Improve and update procedures
OP-16: Security Operations Centre (SOC)
OP-17: Define alerting procedures and communication plan
OP-18: Incident reporting and continuous improvement

Control and auditing

OP-19: Cybersecurity audits
OP-20: Periodic reviews

IT and OT physical protection

OP-21: Physical protection for safety
OP-22: Maintenance operations traceability

SECURITY MEASURES - TECHNICAL

Network security
TP-01: Network segmentation
TP-02: Regular network scans
TP-03: Perimetric security

Access control
TP-04: Centralised tools for IAM
TP-05: IAM strategy
TP-06: Restrict generic accounts
TP-07: Password complexity policies/rules
TP-08: Multi-factor authentication
TP-09: Physical/remote access control
TP-10: Accounts and access right reviews

Administration and configuration management
TP-11: Installation and configuration policy
TP-12: Administrators accounts
TP-13: Privilege Account Management
TP-14: Dedicated administration networks

Threat management
TP-15: Anti-malware, anti-spam and anti-virus

Cloud security
TP-16: Cloud security assessment method
TP-17: Security / availability in cloud SLAs
TP-18: Cloud options for detection/response

Machine-to-machine security
TP-19: Secure M2M exchanges
TP-20: Secure communication protocols

Data protection
TP-21: Cryptography
TP-22: Anonymise / secure personal data

Update management
TP-23: Define update management process
TP-24: Software/firmware authenticity
TP-25: Verify the source of updates

Detection and monitoring
TP-26: Monitor availability of the port systems and devices
TP-27: Logging system
TP-28: Log correlating and analysis systems

Security measures specific for OT systems
TP-29: OT systems in security measures
TP-30: Network segmentation between IT/OT
TP-31: Specific security measures for IoT

Backup and restore
TP-32: Set up backups and ensure they are regularly maintained and tested

BEYOND GOOD PRACTICES!

Awareness raising

At board level and staff level to increase the strategic attention paid to cybersecurity risks, result in higher investment and more resources, and improve cybersecurity in day-to-day operations in ports.

Information sharing

Amongst port operators (port authorities, terminal operators etc.) and between port operators and other maritime stakeholders, such as shipping companies.

Secure supply chain

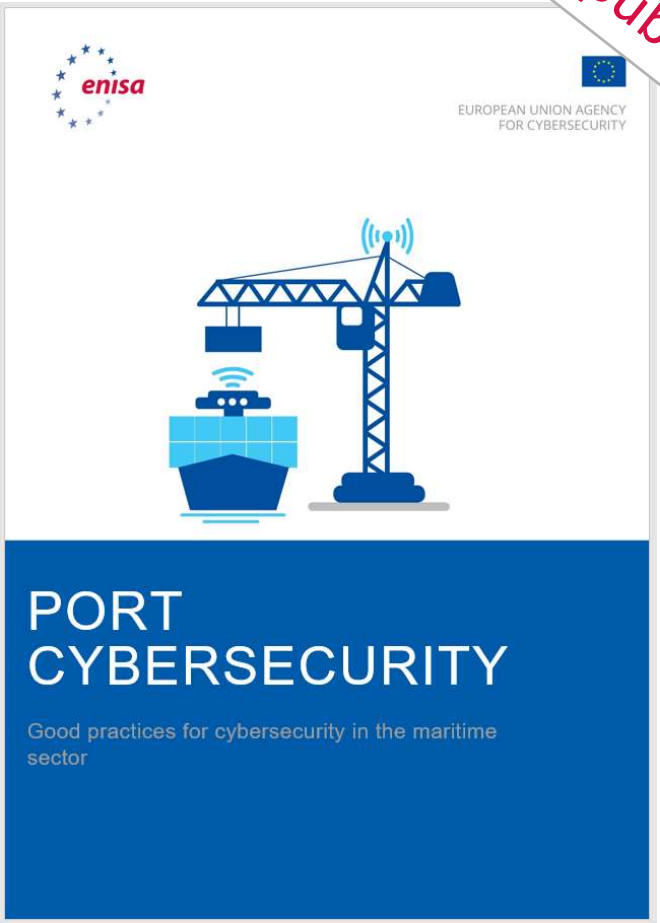
cybersecurity certification of critical components, well-defined supplier obligations for the entire lifecycle of products/services, specific provisions for supply chain management and more.

Interdependencies

Integrate interdependencies cybersecurity risks in the overall cyber risk management process to account for the multiple and complex interconnections of ports with other sectors.

ANY COMMENTS?

Just published!



- Who
- What
- Why
- How

DISCUSSION ON ENISA'S FUTURE ACTIVITIES IN MARITIME

WHAT NEXT?

ENISA 2020 Report on Maritime Cybersecurity

- Topics
- Target audience
- Stakeholders
- Objectives / needs?

2nd Maritime Cybersecurity Workshop

- Workshop or Conference?
- Combined activities?
- Stakeholders/attendees
- Themes / topics / sessions
- Where?

Other activities?

- Trainings / exercises
- Sectorial ISAC
- IMO
- Situational analysis reports / incidents
- Collaboration with EMSA, DG MOVE, MARSEC etc.?
- Support other sectorial activities

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu