

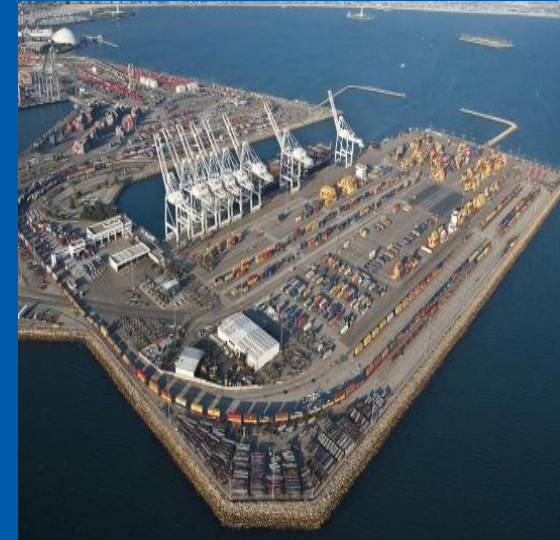


EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY IN MARITIME AND ENISA'S RELATED ACTIVITIES

Dr. Athanasios Drougkas
Cybersecurity Expert
ENISA – The EU Agency for Cybersecurity

8th ShipIT Conference
27 | 09 | 2022

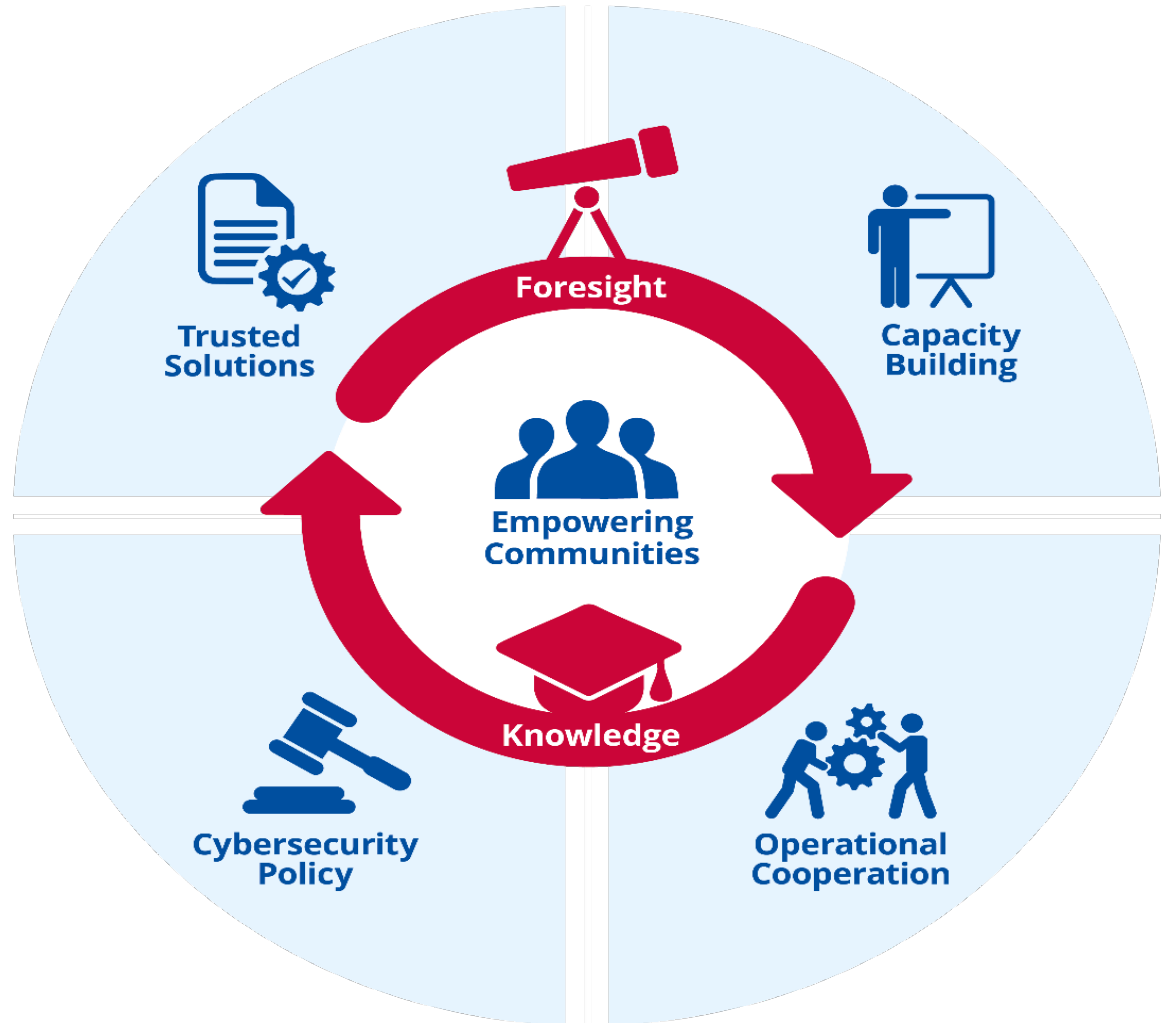




EUROPEAN UNION AGENCY
FOR CYBERSECURITY

A TRUSTED AND CYBER SECURE EUROPE

Our mission is to achieve a **high common level of cybersecurity** across the Union in cooperation with the wider community



RECENT INCIDENTS IN MARITIME

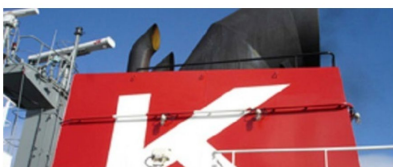
Bureau Veritas hit by cyber attack



Cyberattack Hits Multiple Greek Shipping Firms



Japan's "K" Line Apologizes for Second Cyberattack in Months



News / CMA CGM hit by cyber attack, but says it's business as usual



All Four of the World's Largest Shipping Companies Have Been Hit By Cyberattacks

(zdnet.com)



12

Posted by BeauHD on Tuesday September 29, 2020 @06:30PM from the shore-based-attacks dept.

An anonymous reader quotes a report from ZDNet:

With today's news that French shipping giant [CMA CGM](#) has been hit by a ransomware attack, this now means that all of the four biggest maritime shipping companies in the world [have been hit by cyber-attacks in the past four years](#), since 2017. Previous incidents included: 1.)

Hurtigruten hit by cyber-attack

by The Editorial Team — December 15, 2020 in Cyber Security



IMO hit by cyber attack

This web site is under maintenance. We are sorry for any inconvenience caused.



[GISIS](#) | [IMODOCS](#) | [Virtual Publications](#) | [eRoster](#)

Shipping's global regulatory body the International Maritime Organization (IMO) has been hit by a cyber attack.

News

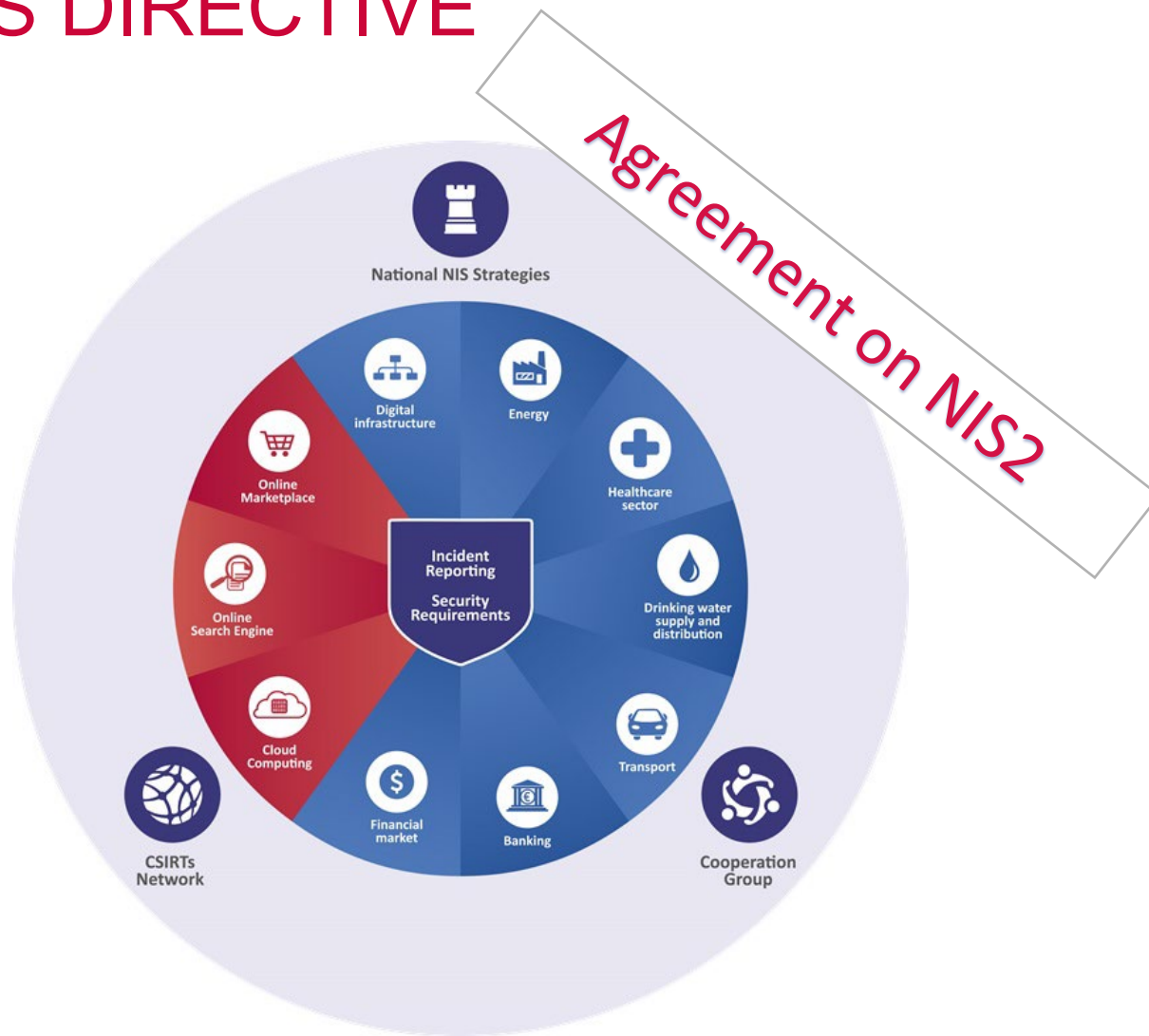
Mediterranean Shipping Company MSC hit by a Cyber Attack

TECH

South Africa port operations halted and workers reportedly put on leave after major cyberattack

PUBLISHED TUE, JUL 27 2021-5:14 AM EDT | UPDATED TUE, JUL 27 2021-6:45 AM EDT

THE NIS DIRECTIVE



NIS2 PROPOSAL – MAIN PILLARS

MEMBER STATE CAPABILITIES



- Identification of National authorities
- National strategies
- **CVD frameworks**
- **Crisis management frameworks**

RISK ASSESSMENT



- **Accountability for top management for non compliance**
- Security measures for companies
- Incident notifications for companies
- European cybersecurity certification schemes

COOPERATION AND INFO EXCHANGE



- Cooperation group
- CSIRTs network
- **CyCLONE**
- **CVD and European vulnerability registry**
- **Peer reviews**
- **Biennial ENISA cybersecurity report**
- **EU registry for some entities (e.g. DNS service providers, TLDs, cloud providers)**

BROADER EU POLICY CONTEXT



CSA



CRA



EUMSS

MARITIME – ENISA PUBLICATIONS



SECURITY MEASURES

POLICIES



Security policy and organisation

Risk and Threats Management

Security and privacy by design

Asset inventory and management

Cyber resilience (Business continuity and crisis management)

ORGANISATIONAL PRACTICES



Endpoints protection and lifecycle management

Vulnerabilities management

Human Resource Security

Third-party management

Detection and Incident response

Control and auditing

IT and OT physical protection

TECHNICAL PRACTICES



Network security

Access control

Administration and Configuration Management

Threat management

Cloud security

Machine-to-machine security

Data protection

Update management

Detection and monitoring

Industrial control systems

Backups and restores

CYBER RISK MANAGEMENT FOR PORTS

Identifying cyber-related assets and services



- Define assessment focus
- Asset inventory
- Map assets to systems
- Map assets to services
- Map assets to information
- Identify 3rd party SW dependencies
- Identify vendor dependencies
- Identify IT/OT dependencies
- Automated asset management
- Cybersecurity in procurement

Identifying and evaluating cyber-related risks



- Risk assessment at enterprise level
- Roles & responsibilities
- Consolidate IT/OT security
- Integrate risk management strategy
- Comprehensive risk likelihood assessment
- Comprehensive risk impact assessment
- Engage in sectorial initiatives
- CTI in risk assessment
- Risk acceptance thresholds
- Cyber risk indicators
- Business impact analysis methodology
- Cyber vulnerability assessment
- Involve senior management

Identifying security measures



- Criteria for implementing measures
- Assess risk reduction effectiveness
- Test security measures via exercises
- Coordinate with asset risk owners
- Security by design
- Align measures with organisational maturity
- Cyber insurance
- KPIs
- Incident response/recovery roles
- Focus incident response on key assets

Assessing cybersecurity maturity



- Ensure inclusive scope
- Cybersecurity awareness and training
- Cybersecurity working group
- Seek advice from external sources
- Cybersecurity programme

ONLINE TOOL ON PORT CYBER RISK MANAGEMENT



This tool allows port operators to conduct cyber risk management with a four-phase approach which follows common principles of risk management. The approach is also compatible with the steps of the risk assessment methodology of the ISPS code. Port operators can navigate through this tool starting at any of the four phases, identify security measures based on their priorities and assess their maturity in the implementation of these measures.

Cyber Risk Management Phases:



Identify cyber-related assets and services



Identify and evaluate cyber-related risks



Identify security measures



Assess cybersecurity maturity

ONLINE TOOL ON PORT CYBER RISK MANAGEMENT

◀ Main
Download ALL (61)
Download Selected (0)

Filter by Assets and/or services (2)

IT Systems X IT end-devic... X

Filter by Threats (2)

Eavesdroppi... X

Expand any security measure to review the examples of implementation for different maturity levels and assess your own maturity.

MEASURES (0 out of 61)	Assets	Threats
<div> <input type="checkbox"/> - PS-01 Information System Security Policy (ISSP) </div> <div> <p>Group: Policies</p> <p>Domain: Security policy and organisation</p> <p>DESCRIPTION</p> <p>Write and implement an information systems security policy (ISSP), which describes all organisational and technical means and procedures, including topics related to the OT environment. This ISSP must be approved by the port's top management team to guarantee the high-level endorsement of the policy. Key elements of the ISSP can be integrated in the Port Facility Security Plan required by the ISPS Code.</p> </div>	<div> <div>Mobile Infrastructure Fixed Infrastructure</div> <div>OT Systems & Networks OT end-devices IT Systems</div> <div>Safety and Security Systems People Information and Data</div> <div>Network & Communication Components IT end-devices</div> </div> <div> <p>EXAMPLES/EVIDENCE FOR ...</p> <div> <p>Maturity level 1</p> <ul style="list-style-type: none"> • The organisation has drafted one or more information system security policies (ISSPs) that provide technical guidance and supporting procedures to stakeholders in protecting information technology and operational technology environments. • The ISSPs include cybersecurity considerations. • The organisation's designated Port Facility Security Officer is familiar with the ISSPs. • The organisation has updated its PSP/PFSP to include ISSPs. </div> <div> <p>Maturity level 2</p> <ul style="list-style-type: none"> • The organisation has formally codified its ISSPs in an overarching plan that provides tailored guidance to stakeholders regarding the organisation's unique IT/OT environment. • Top management have reviewed and approved the organisation's ISSPs. • The updated PSP/PFSP includes a cybersecurity appendix (or annex) that includes all relevant ISSPs addressing cybersecurity considerations. </div> <div> <p>Maturity level 3</p> <ul style="list-style-type: none"> • The organisation regularly reviews its ISSPs to ensure that policies and procedures accord with defined objectives. • The organisation includes ISSP elements within quarterly drills and annual exercises to align security activities with IT/OT operating environments. • The organisation shares its ISSPs with key stakeholders across the organisation. </div> </div>	

OTHER ENISA ACTIVITIES IN MARITIME

Collaboration



Transport TL



EM-ISAC



Community building



THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity

Agamemnonos 14, Chalandri 15231

Attiki, Greece

 +30 28 14 40 9711

 info@enisa.europa.eu

 www.enisa.europa.eu

