MARITIME CYBERSECURITY – BEST PRACTICES FOR VESSELS

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI

www.huoltovarmuus.fi

Security of supply refers to society's ability to maintain the basic economic functions required for ensuring people's livelihood, the overall functioning and safety of society, and the material preconditions for military defence in serious disruptions and emergencies.

The National Emergency Supply Agency (NESA) is an organisation operating under the Ministry of Economic Affairs and Employment. It is tasked with planning and measures related to developing and maintaining security of supply.

The National Emergency Supply Agency operates in conjunction with the National Emergency Supply Council as well as individual sectors and pools that operate as permanent cooperation bodies. Together they form the National Emergency Supply Organisation.

Commissioned by the Finnish National Emergency Supply Organization, The Maritime Transport Pool and Finnish Shipowners' Association

Author:	Deductive Labs Ab
Publisher:	Finnish National Emergency Supply Organization, The Maritime Transport Pool
Images:	Shutterstock
Layout:	Up-to-Point Oy
Year of publication:	2021
ISBN:	978-952-7470-02-2

Table of contents

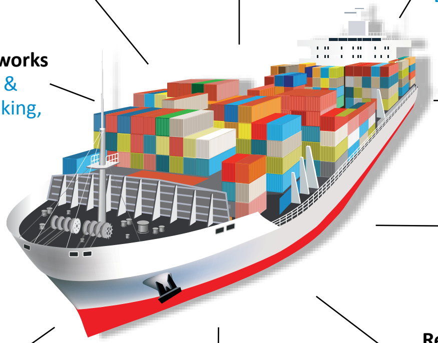
The different steps and best practices for on-board vessel cyber-security are proposed and presented in this document as follows:

BACKGROUND AND INTRODUCTION

Maritime environments and vessels may seem like unusual targets for cyber-attacks, but with the increasing digitalization of the maritime environment and the increased use of network-connected information technology (IT), operational technology (OT) systems, industrial control systems (ICS) and satellite communications, the maritime environments are susceptible to attacks by cybercriminals and other threat groups. It is therefore critical that cybersecurity is properly managed in the maritime environment in order to protect the vessels, crew and cargo against potential cybersecurity threats and attacks.

Maritime cybersecurity is the selection of policies, guidelines, procedures, security controls and measures, risk management actions, best practices, training, tools, and technologies used to protect maritime organisations, their environments, and their vessels.

The risks with IT and OT assets are different in that IT asset risks mainly affect finance and reputation whereas OT asset risks can affect and threaten life, property and the environment if such risks were to materialise.



ICS,
PLC, HMIs, Electrical system
Session hijacking, Eavesdropping, DDoS, Data manipulation

Network Security
Vulnerability exploitation, DDoS

Communications
Session hijacking, System breach, Eavesdropping, Data manipulation, DDoS

Vendor equipment and networks
Malware infection, Network & system breach, Session hijacking, Eavesdropping

Navigation
System takeover, Data manipulation, DDoS

Ship networks
Malware infection, Network & system breach, Session hijacking, Eavesdropping

Physical Security
Social Engineering, Tailgating, Physical breach of perimeter

Remote Administration
Session hijacking, Network breach, DDoS

Crew network
Malware infection, Ransomware, Network & system breach, Session hijacking, Eavesdropping

Cargo Management
Malware infection, Network & system breach, Data extraction/manipulation

In January 2021 the Finnish Shipowners association together with the National Emergency Supply Agency in Finland initiated a project order to map the situation of cybersecurity within the Finnish maritime industry. Deductive Labs Ltd, a Finnish maritime cybersecurity specialist, was engaged to carry out the project.

The project presented three separate documents, available through the Finnish Shipowners' Association and National Emergency Supply Agency webpages: *https://www.huoltovarmuuskeskus.fi/julkaisut* and *https://shipowners.fi/vastuullisuus/turvallisuus/kyberturvallisuus/*

1. ***Maritime Cybersecurity Report – Finnish Maritime Fleet Maturity,*** an extensive report on the current state of the Finnish maritime sector

2. ***Maritime cybersecurity – Best practices for vessels,*** a summary of findings and presentation of best practices for vessels

3. ***Maritime cybersecurity – Best practices for shipowner organisations,*** a summary of findings and presentation of best practices for shipping organisations

1. RISKS FOR CRITICAL SERVICES AND FUNCTIONS ONBOARD VESSELS

- Identify all critical services and functions on the vessels(navigation, propulsion, stability, ballast, etc.)
- Identify all IT-and OT-assets (computers, networks, control and automation systems, bridge systems, navigation, propulsion and machinery, etc) providing these critical services
- Identify risks and their impacts on all identified critical services and assets
- Create a risk treatment plan with actions to remediate or minimise identified risks
- Update list of assets and the risk assessment whenever there are changes

Tips:

Use established risk management procedures from existing ISM/ISPS procedures if applicable or refer to DCSA Asset Management and Risk Assessment Templates:

- DCSA Asset List Risk Assessment Framework examples
- DCSA Asset Management and Risk Register Templates Reading Guide

Outcomes:

- An inventory of the vessel's critical services and functions
- An inventory of the organisation's IT and OT assets and their risks
- The organisation's and the vessels support compliance with the IMO MSC.428(98) resolution
- The risk treatment plan will outline the next steps needed for securing the vessel in order to remediate the identified risks.

Responsibility:

- Key roles and crew members responsible for vessel IT- and OT-systems
- Roles responsible for IT- and cybersecurity

Things to consider:

❑ *Ships networks and computers*
❑ *Bridge systems*
❑ *Cargo handling and management systems*
❑ *Propulsion and machinery management and power control systems*
❑ *Access control systems*
❑ *Passenger servicing and management systems*
❑ *Passenger facing public networks*
❑ *Administrative and crew welfare systems*
❑ *Communication systems*

2. NETWORK SEGMENTATION

The critical systems and assets used on the vessels should be segmented to different networks in order to protect them and restrict any potential breaches or attacks. Network segmentation is a standard principle used in critical networks and one of the key controls in standards such as ISO27001 and ISA/IEC62443.

1. Identify all critical systems and assess the current network design and segmentation
2. Create networks for the different groups of critical systems, such as communication, bridge, engine, cargo, business, crew and wi-fi networks.
3. Move the systems to the segmented networks and update firewall policies accordingly (Step 3)

Tips:

Use standards such as ISO27000 or ISA/IEC 62443 for more information regarding segmentation and using security zones / conduits to increase cybersecurity resilience for critical assets. Create network diagrams for vessels to have a readily accessible visualisation of networks and systems. Start with segmenting the "easiest" networks , such as crew and guest networks before proceeding to segment critical operations networks and assets. Combine similar systems and assets to the same network based on system functionality and criticality, but make sure to avoid over-segmentation that will be counterproductive for the task.

The goal is to ensure that the vessel's critical networks and systems are properly protected from less secure networks, such as passenger, crew, supplier and other untrusted networks.

Outcomes:

- Critical IT- and OT-assets (bridge, engine, etc.) will be segmented into separate networks

Responsibility:

- Key crew members responsible for vessel systems and assets
- Organisation IT, Network and Cybersecurity resources

Things to consider:

Network segmentation for vessel networks:

❑ *Business networks*

❑ *Crew networks*

❑ *Wifi networks*

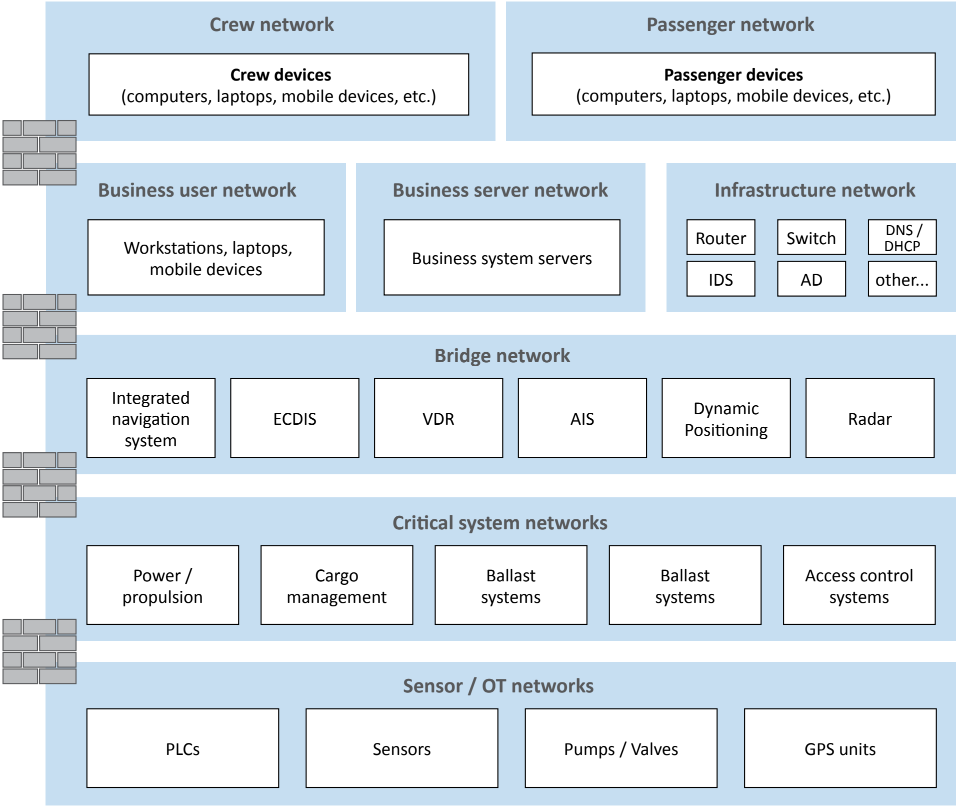
❑ *Passenger networks*

❑ *Engine, power and other machinery networks*

❑ *Supplier networks*

❑ *Other networks as necessary via risk analysis*

Example vessel network segmentation diagram:



Crew network

Crew devices
(computers, laptops, mobile devices, etc.)

Passenger network

Passenger devices
(computers, laptops, mobile devices, etc.)

Business user network

Workstations, laptops, mobile devices

Business server network

Business system servers

Infrastructure network

Router

Switch

DNS / DHCP

IDS

AD

other...

Bridge network

Integrated navigation system

ECDIS

VDR

AIS

Dynamic Positioning

Radar

Critical system networks

Power / propulsion

Cargo management

Ballast systems

Ballast systems

Access control systems

Sensor / OT networks

PLCs

Sensors

Pumps / Valves

GPS units

3. FIREWALL CONFIGURATIONS

When systems have been segmented it is critical that appropriate firewall policies are applied to the networks and systems that only allow approved and necessary traffic to and from the systems.

1. Ensure that all systems and networks are properly protected. Allow only necessary access and avoid granting access to public, unapproved sources. Pay special attention to vessel communication systems (VSAT, Fleet broadband, etc.) and protect them properly by filtering communication, segmenting the systems and applying secure configurations (see step 8 – system hardening
2. Identify the IP-addresses and network communication protocols and data flows needed for the affected assets to function properly.
3. Analyse firewall policies and ensure that only necessary communication is allowed to and from the assets
4. Configure firewalls with a default-deny configuration that blocks and logs all non-approved network communication

Tips:

Use the identified system and asset groups and network and data-flow diagrams created during the network segmentation (step 2). Ensure that proper firewall policies are created for the systems and networks based on the system communication requirements.

Outcomes:

- Firewalls policies are properly configured and applied to only allow necessary traffic to and from the segmented critical systems

Responsibility:

- Key crew members responsible for vessel systems and assets
- Organisation IT, Network and Cyber-security resources

Things to consider:

❑ *Vessel firewalls*
❑ *Segmented networks and assets*

4. REMOTE ACCESS TO CRITICAL SYSTEMS AND NETWORKS

Most vessels rely on multiple third-parties and suppliers for the operation of their critical systems and assets. It is important to control remote and local supplier access to critical systems for both third-parties and internal users.

1. Identify third-parties and internal users that have a requirement to access critical vessel systems
2. Identify and document what IP-addresses, network ports/services and systems that they need access to
3. Update firewall policies to grant third-parties and internal users access to the systems and assets and services they need
4. Document all remote-access connections and ensure that the appropriate remote access agreements are in place
5. Control supplier's local access to vessel's critical systems and networks. Ensure that the suppliers do not connect unsecure devices to vessel networks and supervise usage if needed

Tips:

Use third-party and supplier documentation to identify system access requirements that can be used in the firewall policies. Create Non-Disclosure / remote access agreements that outline the company requirements for accessing vessel networks (VPN connections, personal users, strong passwords/MFA, anti-malware protection on computers, etc.).

Outcomes:

- Remote access to the vessel's critical systems and networks will be controlled
- Agreements for remote access have been established with third-parties and suppliers

Responsibility:

- Key crew members responsible for vessel systems and assets
- Organisation IT, Network and Cybersecurity resources
- External suppliers and third parties

Things to consider:

❑ *List of third parties and suppliers*

❑ *Critical systems managed by third parties or suppliers*

❑ *Instructions for suppliers*

5. MALWARE PROTECTION

Malware protection is a basic component for cybersecurity. Malware protection and end-point-protection-and-response (EDR) solutions are recommended as they both protect the systems as well as provide advanced monitoring and response capabilities in the event of a malware infection.

1. Install and configure malware protection tools on all critical systems where possible (Windows, Linux, MacOS)
2. Ensure that the malware protection tools are regularly and automatically updated
3. Identify systems where malware protection cannot be installed and create alternative controls for these systems (network segmentation, strict access controls, etc). For example ECDIS systems are typically type-approved and ad-hoc installations are not allowed and different protection measures are needed
4. Ensure that all external USB and similar devices are checked for malware before use on the vessel's critical systems

Tips:

Ensure that all systems have anti-malware protection installed in order to protect them from malware threats. This includes emails, websites and USB drives that are accessed and used on the vessel.

Outcomes:

- Malware protection is implemented on all vessel systems and assets where possible
- Systems that cannot be implemented with malware protection have been identified and alternative controls have been identified and implemented to protect these systems against malware

Responsibility:

- Key crew members responsible for vessel systems and assets
- Organisation IT, Network and Cybersecurity resources

Things to consider:

❑ *Ensure that malware protection systems are regularly updated*

❑ *Ensure that malware protection system events are logged, analysed and responded to*

6. LOGGING AND MONITORING

Monitoring and logging are necessary in order to monitor and detect cyberattacks on the network and assets. Without proper monitoring and logging capabilities, it is very difficult to detect attacks and respond to them.

1. Install monitoring and logging solutions for vessel IT- and OT-assets
2. Configure all IT and OT assets to monitor and log to a centralised solution
3. Configure logging for firewalls and other network devices
4. Continuously analyze the logs in order to detect attacks

Tips:

There are many log management solutions available on the market that can be used. Logging and analytics services can be outsourced to a trusted partner that has the knowledge and capabilities to deliver a log analytics service.

Outcomes:

- The vessel critical systems will be monitored and logs are sent to a centralised solution for analysis

Responsibility:

- Key crew members responsible for vessel systems and assets
- Organisation IT, Network and Cyber-security resources

Things to consider:

❑ *All IT systems on the vessels*

❑ *OT systems that have the capability to log*

7. REGULARLY UPDATE ALL SYSTEMS

The most common method for attackers is to exploit vulnerabilities in systems and applications in order to gain access. Therefore it is important to regularly update all systems and applications in order to secure the systems so the vulnerabilities cannot be exploited by potential attackers.

1. Monitor published vulnerabilities from suppliers for all systems and applications
2. Update all systems and applications on a regular basis to fix vulnerabilities
3. Pay special attention to systems and applications that are exposed to untrusted networks or the Internet and ensure that these systems are regularly patched
4. Document patching procedures and responsibilities and ensure that systems are updated in a controlled manner whenever possible(in dock, in harbour, at sea, etc.)

Monthly patch updates are recommended but ensure that the IT teams have the capability to install critical patches quickly if needed.

Tips:

Patching systems and applications can be hard and time consuming, especially if the work has to be done manually. Use automation tools and scripting to help with patching systems in a centralised and automated way. Automation reduces the human resources needed and ensures a standardised method to deploy patches.

Outcomes:

- Systems and applications used on the vessels are patched

Responsibility:

- Key crew members responsible for vessel systems and assets
- Organisation IT, Network and Cybersecurity resources
- External suppliers and third parties

Things to consider:

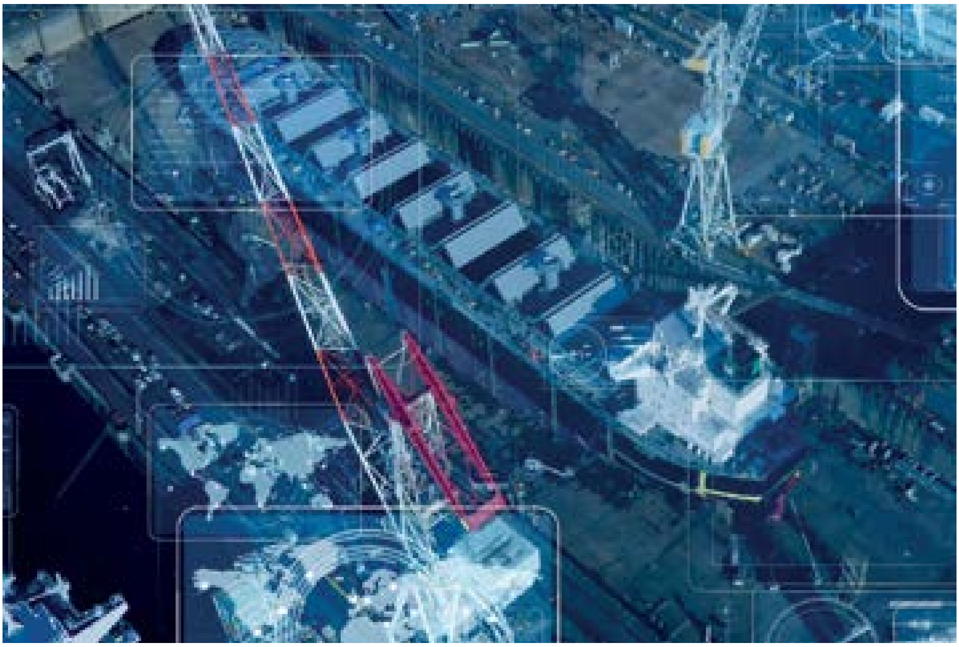
❑ *Patching procedures depending on system criticality*

❑ *Communication regarding patching procedures with persons responsible for the system (internal, supplier)*

8. SYSTEM HARDENING

System hardening is the process of ensuring that all systems and applications are properly and securely configured according to best practices. This includes securing administrative user passwords, configurations, used network protocols (telnet vs ssh), network segmentation, etc.

1. Change all default admin passwords on vessel systems (Satcom, Navigation, Engine control systems, Serial-to-IP converters, etc.)
2. Ensure that all onboard Wi-Fi networks are properly secured and configured with strong passwords and protocols
3. Secure USB ports. Ensure the use of dedicated and secure USB devices if such devices are needed. Check USBs for malware before plugging in to critical systems
4. Do not plug in any personal, unsecure devices to vessel systems or operational networks. Use only designated crew networks
5. Create standard configurations for all systems and applications that take cybersecurity into account
6. Deploy the standardised configurations to the systems and applications
7. Create checklists with actions for new systems (change default passwords, configure secure settings, etc.)
8. Ensure that the vessel's critical systems are properly secured according to vendor instructions(ECDIS, Integrated bridge systems, Radar, AIS, GPS, etc.)



Tips:

Use tools for creating central repositories for configurations and use automation tools and scripting to help with configuring systems in a centralised and automated way. The standardised configurations ensure, for example, that standard passwords are changed and that secure configurations and protocols are used.

Pay special attention to the vessel's critical systems such as ECDIS, Integrated bridge systems, Radar, GPS, etc. which provide critical functions to the vessel, and ensure that proper procedures exist for securing these systems from attacks, jamming and spoofing.

Outcomes:

- Standardised and secured configurations are created that can be used for all systems and applications in the fleet
- Configurations are deployed to systems and applications in a centralised way

Responsibility:

- Key crew members responsible for vessel systems and assets
- Organisation IT, Network and Cybersecurity resources
- External suppliers and third parties

Things to consider:

❑ *Supplier systems can be hard or impossible to automate*

❑ *Ensure that suppliers follow company established requirements and procedures for their systems*

9. SUPPLIER CYBERSECURITY

Most vessels rely on multiple third-parties and suppliers for the operation of their critical systems and assets. It is important to know which third parties and suppliers are used on the vessel and to ensure that they have appropriate cybersecurity controls in place. The agreements should include cybersecurity requirements and the responsibilities they need to adhere to in the delivery of their service.

1. Create cybersecurity requirements for third parties and suppliers that ensure that their delivery is secure.
2. Demand that third parties and supplier systems are secure
3. Ensure that external parties and suppliers are supervised when working with critical systems

Tips:

Cybersecurity is usually said to be as secure as the weakest link. Supplier cybersecurity is therefore important and needs to be managed in order to ensure that cybersecurity is properly managed, Ensure that cybersecurity requirements and responsibilities are documented and that suppliers are informed.

Outcomes:

- The third-parties and supplier agreements include cybersecurity requirements needed to secure their delivery to the vessels

Responsibility:

- Organisation IT, Network and Cybersecurity resources
- Marine operations
- External suppliers and third parties

Things to consider:

❏ *All third parties and suppliers used on the vessel*

10. CYBERSECURITY AWARENESS TRAINING

Training and cybersecurity awareness is crucial to the whole organisation, from senior management to employees and crew. In order to have a basic understanding of cybersecurity and how it affects the vessel, the crew should get training in cybersecurity. This ensures that they have knowledge of what cybersecurity is and what they should do in order to protect the vessel.

1. Organise cybersecurity training for the crew
2. Provide customised and relevant training for different roles in the crew
3. Conduct cybersecurity training regularly
4. Establish cybersecurity training as a continuous part of the company's process and culture

Tips:

Use external training suppliers and online platforms to deliver regular cybersecurity training to the crew

Outcomes:

- Increased understanding of cybersecurity for all employees
- Compliance with IMO guidelines on cyber risk management

Responsibility:

- Organisation cybersecurity resource.
- Vessel masters

Things to consider:

❑ *Provide training to all employees, including senior management*
❑ *Customised and relevant training for different roles*

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI