MARITIME CYBERSECURITY – BEST PRACTICES FOR SHIPOWNER ORGANISATIONS

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: 978-952-7470-06-0

Table of contents

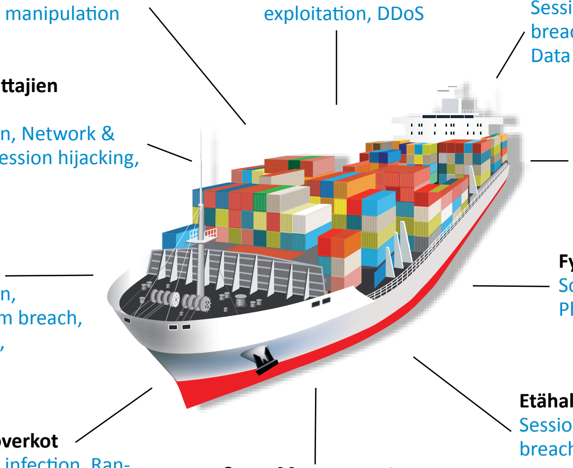
The different steps and best practices for shipowner organisations are proposed and presented in this document as follows:

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 for attacks by cybercriminals and other threat groups. It is therefore critical that cybersecurity is properly managed in the maritime organisation to protect the organisation, 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 would materialise.



ICS, PLC, HMI ja sähkö järjestelmät
Session hijacking, Eavesdropping, DDoS, Data manipulation

Verkkoturvallisuus
Vulnerability exploitation, DDoS

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

Järjestelmätoimittajien laitteet ja verkot
Malware infection, Network & system breach, Session hijacking, Eavesdropping

Navigaatio
System takeover, Data manipulation, DDoS

Aluksen verkot
Malware infection, Network & system breach, Session hijacking, Eavesdropping

Fyysinen turvallisuus
Social Engineering, Tailgating, Physical breach of perimeter

Etähallinta
Session hijacking, Network breach, DDoS

Miehistöverkot
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 cluster. 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. SENIOR MANAGEMENT SUPPORT

Senior management support is critical in order to successfully implement cybersecurity in your organisation. These recommended actions help you get senior management support for cybersecurity

Actions:

1. Engage top management in cybersecurity and include cybersecurity on their agenda
2. Include cybersecurity in the decision-making process
3. Use risk management as an everyday tool for decision-making
4. Educate top management in cybersecurity

Outcomes:

- Increased understanding of cybersecurity and risks to the organisation
- Decisions are made based on information from risk assessments
- Top management lead by example and show cybersecurity is a priority

Tips:

The Finnish National Cyber Security Centre (NCSC-FI) has published cybersecurity guidelines for top management that can be used to increase understanding

- *https://www.kyberturvallisuuskeskus.fi/en/publications/cyber-security-and-responsibilities-boards*
- *https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_ENGdigi_auk280120.pdf*

2. CYBERSECURITY AWARENESS TRAINING

Training and cybersecurity awareness is crucial to the whole organisation, from senior management to employees and crew.

Actions:

1. Organise cybersecurity training for all employees
2. Conduct cybersecurity training regularly
3. Establish cybersecurity training as a continuous part of the company's process and culture

Outcomes:

- Increased understanding of cybersecurity for all employees
- Support compliance with IMO guidelines on cyber risk management[1]
- Organisational cybersecurity awareness is increased

Tips:

If your organisation has dedicated cybersecurity resources, they can be used to create training materials for your organisation. Cybersecurity training should be provided to all employees, even senior management. Different roles need different approaches so consider providing training that is customised for the specific roles and their specific cybersecurity challenges and needs.

External resources and web-based training can be used to provide the training.

[1] https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

3. CYBERSECURITY PROCEDURES AND INSTRUCTIONS

The organisation's employees and vessel crew need to have clear and concise procedures that define how cybersecurity is managed in the organisation and on the vessels.

Actions:

Create the following practical procedures, guidelines and instructions for the crew:

1. how to use systems and services
2. how to manage external media
3. how to update and manage systems
4. how to use personal devices, networks and Internet
5. Instructions for supplier remote access
6. Guidelines for cybersecurity incident management
7. Instructions for cybersecurity exercises

Outcomes:

- The organisation's employees and vessel crew will have documented procedures on how cybersecurity is managed in the organisation and on the vessels
- The organisation and vessel cybersecurity procedures support the requirements from ISM/ISPS

Tips:

Collaborate with employees, crew, suppliers and other third parties to understand the daily operations and how their activities affect cybersecurity in the organisation and on the vessels. Include the parties in the development of practical procedures that are easy to understand and follow.

Creating a cybersecurity culture is the responsibility of senior management.

4. CRITICAL SERVICES AND FUNCTIONS IN THE ORGANISATION

Identifying and understanding the critical services and functions used in the organisation and on its vessels is critical to understanding and maintaining cybersecurity. The organisation needs to identify all the critical services and functions and the related IT- and OT-assets in order to identify the risks and potential impacts to the delivery of the services in case of a cybersecurity incident. This includes all services and functions used in the organisation, both on land and on the vessels.

Actions:

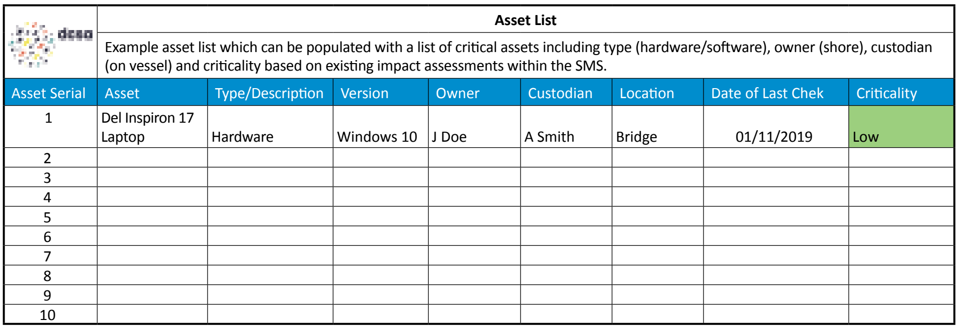
1. Identify and document all critical services and functions in the organisation
2. Identify and document all IT and OT assets related to the delivery of the critical services and functions
3. Start with basic tools, such as spreadsheets and documents and consider implementing automated tools for asset discovery to make the process more efficient

Outcomes:

- The organisation's critical services and functions are inventoried
- The organization's IT and OT assets are inventoried. This includes both organisational systems as well as vessel systems
- The inventory can be used in the risk management process

Tips:

Asset management and creating asset inventories can be labour-intensive tasks. We recommend starting with DCSAs "***Asset Management and Risk Register Templates Reading Guide"*** [2] which includes usable templates to get started with creating asset inventories and risk management. Start by identifying and documenting critical systems and functions and their related assets with a potentially high impact on the organisation or vessel operations and safety.



Asset List

Example asset list which can be populated with a list of critical assets including type (hardware/software), owner (shore), custodian (on vessel) and criticality based on existing impact assessments within the SMS.

Asset Serial	Asset	Type/Description	Version	Owner	Custodian	Location	Date of Last Chek	Criticality
1	Del Inspiron 17 Laptop	Hardware	Windows 10	J Doe	A Smith	Bridge	01/11/2019	Low
2								
3								
4								
5								
6								
7								
8								
9								
10								

[2] https://dcsa.org/wp-content/uploads/2020/03/DCSA_Asset-Management-and-Risk-Register-Templates-Reading-Guide.pdf

5. RISK ASSESSMENT

When the organisation's critical services and their related IT- and OT-assets have been identified and documented, a risk assessment should be carried out to identify threats, risks and vulnerabilities related to the assets that can negatively impact the organisation and vessel operations and safety.

Actions:

1. Assess cybersecurity risks and their impacts for the identified services and related assets
2. Identify and document actions needed to manage the identified risks
3. Create an action plan from the actions identified in the risk assessment
4. Reference the cybersecurity risk management policy from the safety management system(SMS)

Outcomes:

- The organisations risks related to the critical services and functions are identified and documented
- An action plan for remediating identified risks is documented
- Support compliance with IMO requirements for cyber risk management for vessels

Tips:

There are many different models and spreadsheets publicly available that can be used to get started with basic risk management. We recommend starting with DCSAs ***"Asset Management and Risk Register Templates Reading Guide"*** [3] which includes usable templates for asset inventories and risk management. As the risk management process matures, other tools can be used.

[3] https://dcsa.org/wp-content/uploads/2020/03/DCSA_Asset-Management-and-Risk-Register-Templates-Reading-Guide.pdf

6. RISK MANAGEMENT PLAN

When critical services, functions and their related assets and risks have been identified the next step is to create an action plan with actions and remediations for managing the identified risks. This step is based on the risk assessments and will outline both procedural and technical controls that need to be implemented to minimise and remediate risks.

Actions:

1. Create a project plan for the items in the action plan
2. Ensure that the project plan identifies the steps and actions needed to remediate the risk, what resources are needed, who is responsible, what the timeplan is and that a budget is approved and allocated
3. Implement the project plan

Outcomes:

- The action plan has been documented and implemented
- The identified risks have been remediated

Tips:

Treat the actions as a project with documented plans and tasks that can be followed up. You do not need to reinvent the wheel, use existing company project management methods and tools to get the work done.

7. CYBERSECURITY ARCHITECTURE

Documented cybersecurity architecture for the organisation and the vessels is needed to describe how cybersecurity is implemented in the organisation and on the vessels. Cybersecurity architecture helps to ensure that cybersecurity controls are documented and implemented in a standardised way in the organisation and on the vessels.

Actions:

1. Create a cybersecurity architecture document that describes how cybersecurity is implemented in the organisation and on the vessels
2. Create specific cybersecurity plans (CSP) for each vessel, based on the cybersecurity architecture and actual technical environment and needs of each vessel
3. Align the cybersecurity plan with documented cybersecurity procedures

Outcomes:

- Cybersecurity architecture has been documented and describes how cybersecurity is implemented in the organisation and on the vessels
- The cybersecurity architecture is used to create cybersecurity plans for each vessel

Tips:

The organisation's cybersecurity architecture describes how cybersecurity is technically implemented in the whole organisation, including the vessels. Each vessel needs to have a cybersecurity plan based on the overall architecture. The vessel cybersecurity plan can be included in existing ship security plans (SSP) but we recommend creating a separate cybersecurity plan (CSP) to keep the documents separate, as the SSP traditionally focuses more on the physical security of the vessels. Adding cybersecurity to the SSP could make it more complex and harder to understand and follow. The cybersecurity plan should be aligned with the documented cybersecurity procedures that have been developed.

8. SUPPLY CHAIN CYBERSECURITY

The maritime sector is highly dependent on various external suppliers and third parties and they have an important role in the management and operation of the vessels. The suppliers usually have a responsibility to manage and monitor critical systems onboard the vessels, such as ECDIS systems, engines and power management, cargo management systems, GPS systems, PLCs, sensors, etc.

Actions:

1. Identify all suppliers
2. Perform supplier risk assessment
3. Create supplier cybersecurity requirements
4. Include cybersecurity requirements in supplier agreements
5. Ensure that the right to audit is included in supplier agreements

Outcomes:

- Suppliers are identified
- Cybersecurity requirements for suppliers are documented
- Cybersecurity in the supply chain is managed

Tips:

Start by identifying and documenting all suppliers that provide systems and services to the vessels. Develop cybersecurity requirements for the suppliers based on the risk assessments that have been done.

Good and actionable guidance on supply chain security can be found in UK NCSC Supply chain security guidance[4].

[4] https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security

9. INCIDENT MANAGEMENT, RESPONSE AND RECOVERY

Effective incident management enables organisations to identify cybersecurity incidents and to quickly respond and recover from the incident so that the impact of the incident does not affect the organisation and the safety of the vessels.

Actions:

1. Create a cybersecurity incident management procedure. The procedure should describe what actions the crew should take in case of a cybersecurity incident, including detection, response and recovery activities.
2. Ensure that the environment is monitored and events are logged to facilitate the detection of incidents
3. Organise cyber exercises to train the employees and crew on how to react in the case of a cyber incident.

Outcomes:

- The organisation can detect, respond and recover from cybersecurity incidents
- Cybersecurity exercises are done regularly

Tips:

Start by creating incident management procedures that describe what the crew should do in the case of a cybersecurity incident on the vessel. The procedures should include how incidents are detected, how response activities are organised and what needs to be done to recover from the incident.

Use NCSC-Fi Guidelines on cyber exercises to get started:

- *https://www.kyberturvallisuuskeskus.fi/en/our-services/exercises*
- *https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Instructions%20for%20organising%20cyber%20exercises.pdf*

Organizing cyber exercises is a good and effective way to train the crew to respond to cyber incidents.

10. CYBERSECURITY STANDARDS AND FRAMEWORKS

The ISO 27001 is a common standard for creating an information security management system (ISMS), however the standard is not fully aligned with the maritime environment requirements. Standards such as the NIST Cybersecurity Frameworks (NIST CSF) and ISA/IEC 62443 Security for Industrial Automation and Control Systems are better aligned and used for cybersecurity in a maritime environment.

Actions:

1. Choose a cybersecurity standard or framework for your organisation
2. Use your risk analysis to identify necessary actions and controls
3. Document cybersecurity policies, processes and procedures based on the chosen framework

Outcomes:

- The organisation uses an established standard or framework for cybersecurity

Tips:

There are many different standards and frameworks available that can be used to guide your cybersecurity efforts, the most popular being ISO 27001, ISA/IEC 62443 and the NIST Cybersecurity framework.

We recommend that your organisation either contacts external resources and specialists or invests some time and effort in getting some insight into the different standards and frameworks available, in order to determine which one is most suitable for your specific environment and needs.

By using established standards, cybersecurity activities become more standardised and easier to implement, maintain and audit.

External experts can be used to implement cybersecurity standards to make work more efficient.

11. COLLABORATE WITH EXTERNAL PARTIES

A final recommendation, if deemed necessary, is to get external help from industry organisations, peers, associations, or experienced partners in cybersecurity that can help with implementing cybersecurity in your environment.

Examples of external organisations are:

- Industry peers
- Maritime organisations and associations
- Classification societies
- Maritime insurance companies
- National cybersecurity authorities
- Cybersecurity consultancies

Cybersecurity is a complex endeavour that requires specialised knowledge that is hard to find. Your IT and OT teams are most likely already working hard with their regular tasks and projects, and it can be easier and cheaper to get help from external resources with previous knowledge of maritime cybersecurity instead of hiring hard-to-find experts in your organisation.

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI