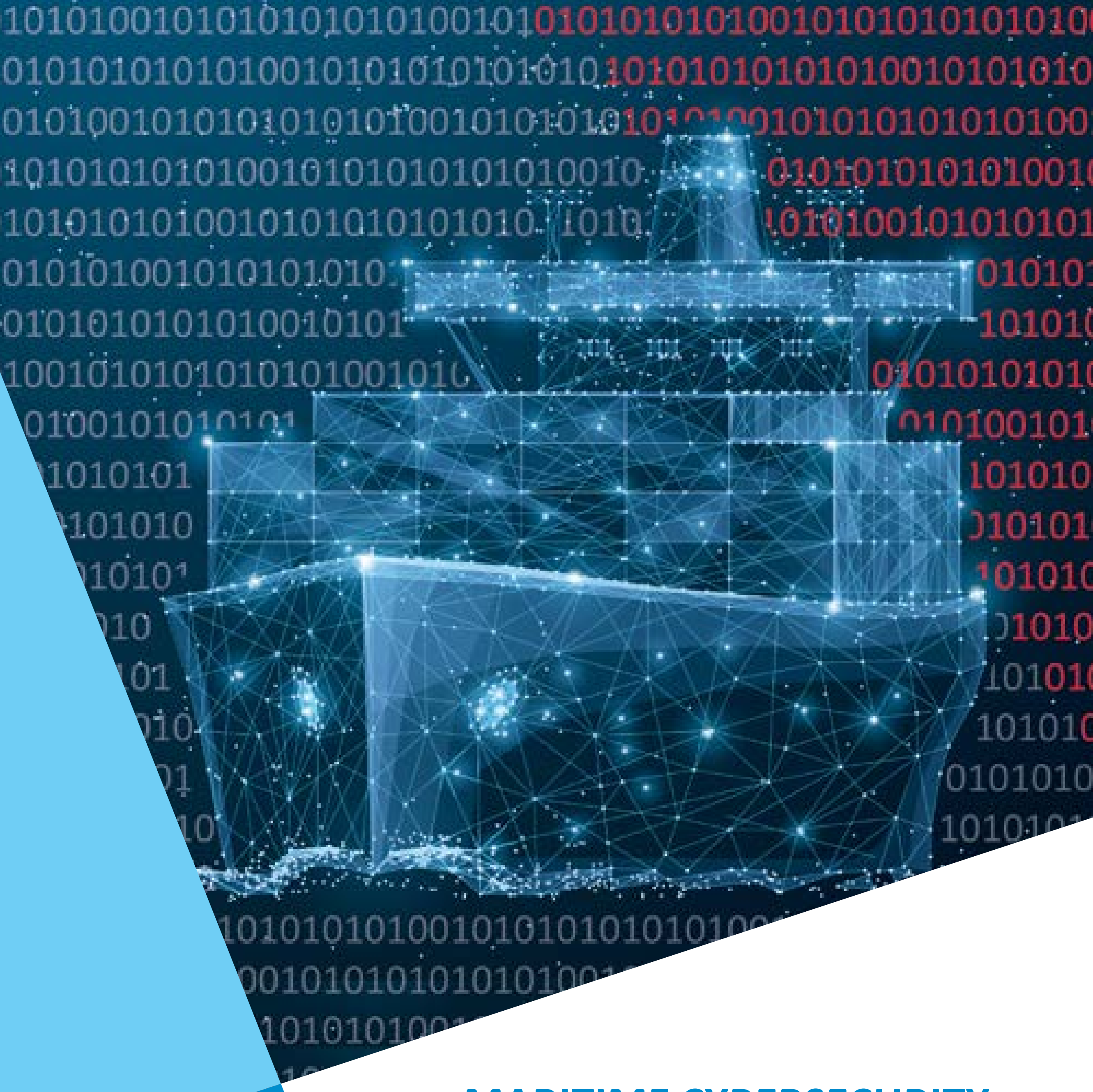


MARITIME CYBERSECURITY REPORT – FINNISH MARITIME CYBERSECURITY MATURITY

Current state report and best practices for the Finnish Maritime sector

Version: 20210603

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI

MARITIME CYBERSECURITY REPORT – FINNISH MARITIME CYBERSECURITY MATURITY

Current state report and best practices for the Finnish Maritime sector

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: 978-952-5608-94-6

Table of contents

1. EXECUTIVE SUMMARY

Cybersecurity is becoming increasingly important for the maritime industry. Maritime environments and vessels may seem like unusual targets for cyber-attacks but cyberattacks are increasingly targeting maritime operators and reports of successful attacks are frequently reported.

The maritime industry regulators have responded to the increasing threats by publishing regulations for cybersecurity, specifically cyber risk management, for the maritime operators. IMO published the resolution MSC.428(98) Maritime cyber risk management in safety management systems in 2017, that requires maritime operators to include cyber risk management in their safety management systems. Cyber risk management procedures must be addressed in the first DOC audit after 1.1.2021.

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:

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

2. *Best practices for on-board vessel cybersecurity*, a summary of findings and presentation of best practices for the onboard activities

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

A survey was conducted as an online survey and sent to 25 members of the Finnish Shipowners Association. The survey was delivered in two parts, one for the organisation and one for the vessels in the organisation.

The organisational survey received 6 responses and the vessel survey received 38 responses. Due to the rather low input from the survey respondent we can see indications and trends but not the total facts and situation regarding cybersecurity in the Finnish fleet.

The survey data shows that the cybersecurity maturity level for the Finnish maritime sector is relatively **low** with an average Maturity level 1 (MIL-1) between all respondents, according to the Cybermeter model.

Based on the responses received, we can see that there is a need for improving cybersecurity in the fleet. Many organisations have implemented basic cybersecurity in their organisation and on the vessels, but there seems to be a general lack of documented cybersecurity governance, specifically with risk management which is required by the IMO resolution MSC.428(98). The lack of cybersecurity governance and risk management indicates a lack of awareness of cybersecurity in the organisation's leadership.

Senior management awareness and support is critical to succeeding with cybersecurity in the organisation. Training and cybersecurity awareness is crucial to the whole organisation, from senior management to employees and crew. Establish cybersecurity training as a continuous part of the company's process and culture.

Furthermore, there is an indication of different approaches and awareness to cybersecurity in the IT and OT areas. It is important for the organisations to ensure that there is a close collaboration between IT- and Maritime operations departments to ensure that cybersecurity is considered in both environments and specifically when connecting operational equipment to vessel networks.

This report presents 10 best practices for shipowner organisations and vessels. Due to the complexity of the shipping organisations and the difference in traditional IT cybersecurity and vessel cybersecurity practices, there are two separate best practices documents:

- *Maritime Cybersecurity – Best practices for shipowners organisations*
- *Maritime Cybersecurity – Best practices for vessels*

The shipowner organisation best practices are more focused on governance and processes and the vessel best practices are focused on more practical activities to be carried out on vessels.

2. BACKGROUND / 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.

In a cybersecurity survey and corresponding whitepaper published by BIMCO and Safety at Sea in 2020[1], the respondents reported that cyber attacks are increasingly seen as a threat to maritime organisations. 38% of respondents indicated they see cyber attacks as a high risk. The survey also found that attacks against maritime organisations are increasing, with 21% of respondents experiencing cyber attacks in 2016 and 31% in 2020. Operational technology (OT) cybersecurity remains a hot topic in the maritime sector and attacks on OT have been reported. In 2019, the US Coast Guard revealed that a large international ship had been the target of a successful malware attack that "significantly degraded the functionality of the onboard computer system"[2].

There have been multiple high-profile breaches in maritime organisations reported in the news over the past few years, from the infamous Maersk NotPetya attack in 2017 to cyberattacks even targeting IMO in 2020.

Even with the IMO regulations requiring documented cyber risk management processes since 1.1.2021, maritime operators are still struggling with establishing cyber risk management practices in their environments. Maritime organisations leadership.

2.1. Report method, survey and interviews

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 maturity and preparedness of the vessels and shipowners. Deductive Labs Ltd, a Finnish maritime cybersecurity specialist, was engaged to carry out the project.

The project activities included an online survey that was conducted among the members of the Finnish Shipowners Association. The survey content was based on the Finnish National Cybersecurity Centre Cybermeter Assessment Tool (Kybermittari arviointityökalu[3]), a national framework for the assessment of cybersecurity capabilities including some details and refinements towards the maritime industry. The survey aims to assess the current state of cybersecurity of the Finnish fleet and shipowners, and present best practices and recommendations for improving the cybersecurity practices.

1) https://ihsmarkit.com/Info/1020/safety-at-sea-and-bimco-cyber-security.html
2) https://nakedsecurity.sophos.com/2019/07/11/cybersecurity-attack-lands-ship-in-hot-water/
3) https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter

The survey was then followed up by in-depth interviews together with a subset of the respondents to get more valuable and accurate information from the survey results and ensure the data and answers are aligned with reality.

3. WHAT IS MARITIME CYBERSECURITY?

The Maritime industry is regulated by different regulations that require maritime operators to ensure the safety and security of vessels.

- SOLAS convention[4]
- ISM Code[5]
- ISPS Code[6]
- EC Regulation 725/2004[7]
- IMO MSC.428(98) Cyber Risk Management in Safety Management Systems
- Port state requirements and controls

These regulations also apply to cybersecurity and with the IMO resolution MSC.428(98), cybersecurity risks now need to be addressed in the safety management system (SMS) and properly documented and addressed in DOC audits after 1.1.2021.

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.

According to the International Maritime Organisation (IMO) Guidelines on Maritime Cyber Risk Management (MSC-FAL.1-Circ.3)[3], maritime cyber risks are defined as:

> *"...maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised."*

Furthermore, the International Safety Management (ISM) Code section 1.2.2 specifies that:

> *"...Safety management objectives of the Company should, inter alia [...] provide for safe practices in ship operation and a safe working environment. [...] assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards; and [...] continuously improve safety management skills of personnel ashore and aboard ships, including preparing for emergencies related both to safety and environmental protection..."*

[4] https://www.imo.org/en/KnowledgeCentre/ConferencesMeetings/Pages/SOLAS.aspx
[5] https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx
[6] https://www.deutsche-flagge.de/de/redaktion/dokumente/dokumente-sonstige/ism-code-engl.pdf
[7] https://eur-lex.europa.eu/legal-content/En/LSU/?uri=CELEX:32004R0725

Many of the existing vessels still use old and legacy systems and technologies that were not built to be connected to the Internet or used in untrusted networks. These systems and networks onboard vessels include a blend of information technology (IT) and Operational Technology (OT) systems. These systems are used by the crew, passengers and third-party suppliers. If not managed properly, the technological environment may expose vessel system vulnerabilities to hackers resulting in compromise of vessel critical operational systems and technologies.

Therefore, it is critical that cybersecurity is properly managed to protect the vessels, their crew and cargo against potential cybersecurity threats and attacks.

3.1. Maritime cybersecurity threats

The maritime sector is increasingly being targeted by cybercriminals and several maritime organisations have reported breaches in the last couple of years. The most known cyber attack in the industry on Maersk in June 2017, estimated to create losses for a value of $300M[8], became a harsh eyeopener for the whole industry. Other examples of maritime cyberattacks are the attacks against Cosco[9], Mediterranean Shipping Company (MSC)[10] and French shipping company CMA CGM[11], which all suffered from ransomware attacks causing disruptions in their operations. Even the International Maritime Organisation (IMO) was hit by a cyberattack in October 2020[12], causing interruption to IMOs website and documents[13].

According to the Threat Landscape Report 2021[14] by CERT-EU, extortion and ransomware attacks are one of the top 10 threats to organisations worldwide, including maritime organisations. Extortion and ransomware attacks are the most disruptive of the identified threats and can cause considerable financial harm and operational impact in case of a successful attack against a maritime organisation.

These cybersecurity threats can target and exploit both traditional organisational IT systems as well as the critical IT and OT systems onboard vessels and can threaten the safety of the vessel and surrounding marine environment. For example, jamming and spoofing attacks against the Global Positioning System(GPS) have been seen in the wild[15] affecting vessel navigation and operations.

Therefore it is clear that cybersecurity must be part of a maritime organisations' risk management approach. The cybersecurity threats can affect both the organisation and its vessels, and appropriate measures should be taken to protect both the traditional organisational IT-systems and the vessel critical operational systems.

[8] https://www.infosecurity-magazine.com/news/maersk-admits-notpetya-might-cost/
[9] https://www.infosecurity-magazine.com/news/cosco-hit-by-suspected-ransomware/
[10] https://gcaptain.com/msc-reports-network-outage-cyber-attack-cannot-be-ruled-out/
[11] https://www.everstream.ai/risk-center/special-reports/cyber-attack-on-cma-cgm/
[12] https://gcaptain.com/imo-cyberattack-has-serious-implications/
[13] https://twitter.com/IMOHQ/status/1311601524209049601
[14] https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf
[15] https://safety4sea.com/cm-understanding-gps-spoofing-in-shipping-how-to-stay-protected

Cybersecurity threats can be malicious or benign. Malicious attacks are activities such as hacking and exploiting vulnerable systems with malware. Benign threats are activities such as inadequate software maintenance, misconfigurations, permissions, weak passwords, etc.

Cyberattacks are generally defined as indirect (untargeted) and direct (targeted). An indirect attack is when your organisation or information is one of many potential targets attacked by using e.g. Malware, Malicious code or Virus, Phishing, Waterholing, Scanning, etc. A direct attack on the other hand is when your organisation is the primary target. In this situation, the methods are generally much more refined and customised and therefore more difficult to protect the company against.

So who are the actual threat actors, and what are their motives?

The common list of threat actors are grouped by different profiles:

- **Cybercriminals:** organised crime groups with considerable resources and knowledge
- **Commercial competitors:** competitors and parties with interest in commercial or other secret information
- **Insiders and individuals:** disgruntled employees and dissatisfied customers when revenge is a rather common motive
- **Hacktivists:** activist groups, often acting on the basis on more ideological terms with varying objectives
- **Terrorists:** extremist groups or non-state actors that use cyber attacks to intimidate, coerce, influence or disrupt a target and force a political change and cause fear or physical harm
- **Nation-states and state-sponsored actors:** government-sponsored groups that target and gain access to networks and systems of other governments or industries to steal, disrupt, damage or change information

The motivations driving these threat actors to attacking maritime environments and vessels can be summarised into the following categories:

- **Political, Ideological, Technical, and Military:** Threat actors like Hacktivists and nation-state and state-sponsored actors are typically motivated by political, ideological and military agendas. They are focused and have an established objective/target in mind when they start planning an attack. This data is seldomly seen for sale on the black market as the motives.
- **Profits/Financial Gain:** Profit and financial motivation is the most common motivations for cybercriminals and sometimes for commercial competitors and insiders. These actors don’t usually care about a specific organisation or business and are just seeking financial gain and aim to convert stolen information and data to money as soon as possible. The victims are usually organisations with a high profile and poor cybersecurity maturity

- **Notoriety/Reputation:** Some threat actors are motivated by reputation, notoriety and attention and will seek targets that help them to gain recognition. The victims are usually organisations with a high profile and poor cybersecurity maturity.
- **Revenge:** Revenge is unfortunately a common threat actor motivation. Among these actors are primarily disgruntled employees and dissatisfied ex-employees, with enough knowledge about an organization's systems, networks, and even defences.
- **Overlap of Motivations:** In many cases there are a overlap of motivations for a threat actor when an attack may be a combination of eg. revenge and financial gain.

3.2. Information Technology (IT) and Operational Technology (OT)

When identifying and analysing technical assets onboard vessels, it is important to be aware of the differences between traditional **Information Technology (IT)** and **Operational Technology (OT)**. The differences, however, do not require that assets should be kept and maintained separately. Traditionally, many businesses have separated OT and IT, but with everything becoming more and more connected and integrated, OT and IT are also moving closer to each other.

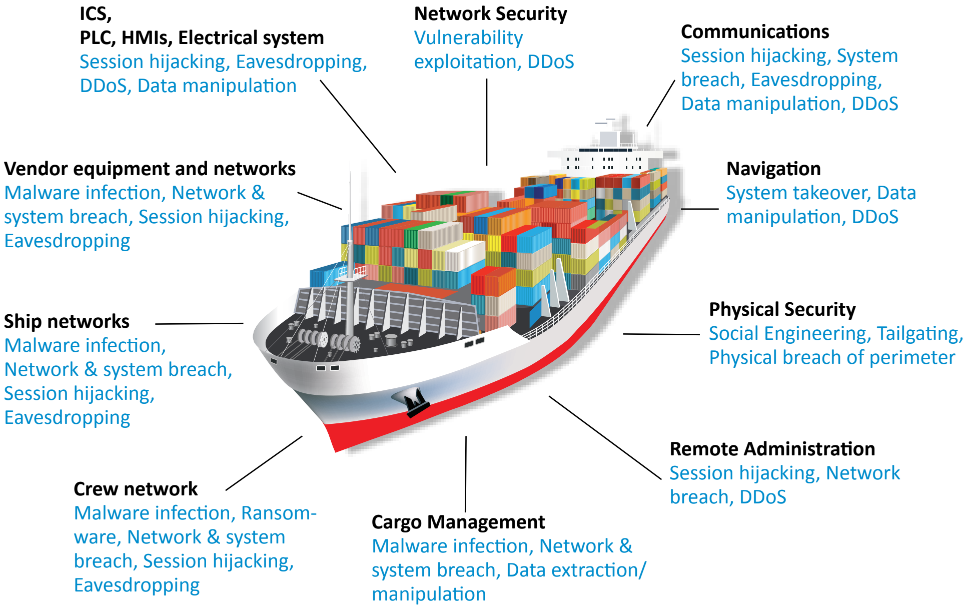
A general difference between the two systems is that while OT systems control the physical world, IT systems manage data. OT refers to the hardware, systems and software that operate your vessels as well as monitors/controls physical devices and processes. IT, then, refers to the technical assets that are used in managing information processing, including software, hardware and communication technologies.

Information Technology (IT) systems in maritime environments comprise of traditional company IT systems that may include:

- Workstations, laptops and mobile
- Mail & calendar
- Intranet, file shares
- Business and financial systems
- Business analytics
- Order management

Operational Technology(OT) systems are the operational systems and equipment onboard vessels. OT systems are usually less well-known than IT systems and often managed by suppliers.

- Navigational (ECDIS, Radar, AIS, GPS, VDR, etc.)
- Communications (Satcom, Fleet Broadband, 3G/5G, Wifi)
- Power management
- Cargo management
- Sensors, PLCs, pumps, actuators, hydraulics, cranes, etc.



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

When it comes to IT and OT systems, each company and organization have different stakeholders or “owners” of the different technologies onboard. Due to the commonly found asymmetry of information between the two, IT and OT departments must cultivate a mutual exchange of knowledge based on well-established communication practices as well as synchronized and harmonized processes and procedures.

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.

NSA recently published an advisory regarding IT and OT system connectivity *“Stop Malicious Cyber Activity Against Connected Operational Technology”*[16] that outlines increasing risks and threats with using and connecting OT technologies to internal networks and the Internet. The advisory comes as a response to the increasing threats against critical infrastructure providers and operators where numerous successful attacks have been reported in the last years, the latest attack being the ransomware attack against the Colonial Pipeline in Texas[17].

> *“This is the largest impact on the energy system in the United States we’ve seen from a cyberattack, full stop,” says Rob Lee, CEO of the critical-infrastructure-focused security firm Dragos”*

The maritime industry operators face similar threats and have to take appropriate actions in their environments and ensure that all IT and OT systems that are connected to internal networks are properly secured.

[16] https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/0/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF
[17] https://www.wired.com/story/colonial-pipeline-ransomware-attack/

3.3. Cybersecurity Governance

Managing cybersecurity in a complex maritime environment is not an easy task and requires good planning and design to ensure that the implementation of cybersecurity controls is done in a standardised and documented manner. This requires that maritime operators establish cybersecurity policies and processes that describe how cybersecurity is managed in the organisation and on the vessels.

For a long time, the senior management and boards of maritime organisations have seen cybersecurity and risk management as a task for the IT department. senior management support and commitment is already required and addressed in the preamble of the ISPS code where the following important statement is made:

> *6. The cornerstone of good safety management is commitment from the top.*
> *In matters of safety and pollution prevention it is the commitment,*
> *competence, attitudes and motivation of individuals at all levels that*
> *determines the end result*[18]*.*

senior management needs to understand this new but equally important area in the operation of vessels. It is therefore required and crucial that the senior management is committed to supporting and funding the cybersecurity efforts in the organisation.

All cybersecurity threats and risks can be effectively managed by informed and detailed planning, implementation, management and monitoring of cybersecurity activities in the organisation and onboard vessels. A cybersecurity risk management culture and mindset need to be instilled in the maritime industry and adopted and implemented in all maritime organisations. The new IMO resolution is a start for a change in the culture of the maritime industry of the future and a necessary step to improve the cybersecurity maturity in the whole maritime industry.

3.4. Cybersecurity Risk Management

Risk management is a crucial part of good cybersecurity governance and is one of the main requirements in the IMO resolution MSC.428(98). It is therefore important that maritime operators document the cybersecurity risk management methodology and perform risk assessments continuously to identify risks and create risk treatment plans to manage and minimise the risks. Traditional risk management is already part of the ISM/ISPS code and implementing cyber risk management should be included in a similar way.

Risk management is one of the core practices needed for cybersecurity in maritime organisations. The risk management practice will identify the needed actions and give the senior management the necessary information to support necessary decisions in the organisation. Furthermore, risk management will provide the organisation and affected departments, teams and employees the necessary actions and controls to be implemented in order to raise cybersecurity maturity and be compliant with applicable regulatory requirements.

[18] https://www.deutsche-flagge.de/de/redaktion/dokumente/dokumente-sonstige/ism-code-engl.pdf

3.5. CASE-STUDY: Ransomware

Ransomware is a malicious attack where attackers encrypt an organisation's data and then demand payment to restore access. Attackers may also steal the organisation's data and demand payment in order to not disclose the data to the competitors, authorities, customers or to the public. There have also been extreme cases, like the Vastaamo case in Finland (*https://vastaamo.fi/en.html*), where the attackers breached a psychiatric clinic and demanded ransom from the company and additionally also sent payment demands for payment to psychiatric customers in order not to disclose the sensitive medical data.

Ransomware attacks disrupt or halt the organisation's operations and is currently one of the top cybersecurity threats. It poses a difficult dilemma for management: pay the ransom and hope the attackers restore the data or try to restore the data themselves. Paying the ransom is not recommended as it gives the criminals incentive to continue their attacks, and the money may be used to fund other forms of crime.

It is important to note that criminals are interested in any systems that are relevant to the target business. As an example, in the case of the widely publicised Colonial Pipeline attack[19], the criminals targeted office networks instead of the actual pipeline network. Even when the oil pipeline systems worked throughout the attack, the operations were affected as systems related to business operations, safety and compliance were taken offline.

This is often the trend with these kinds of attacks. In many cases, the criminals try to attack essential support systems, which are typically internet-connected and have connections to other systems. These could include customer and billing related systems, or systems related to inventory or other enterprise resource handling. Criminals usually try to make sure that any connected backup systems are attacked at the same time to hamper recovery. In other cases, backups have proved to be too old to be useful or the untested recovery processes have not worked.

The methods typically used to gain access to the organisations data are commonly used attack methods, from exploiting vulnerabilities in unpatched systems to tricking users to executing ransomware programs. These malicious ransomware programs then spread laterally on the network by exploiting vulnerabilities in unpatched systems, encrypting all data in its path.

[19] https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/

According to some reports, there is no guarantee that an organisation will not be attacked again even after paying the ransom. According to a industry report[20], half (50%) of ransomware victims were breached again even after paying the ransom.

Fortunately, organisations can plan and prepare for these types of attacks and minimise the risk of successful ransomware attacks against the organisation and its data. The steps include identifying and protecting critical systems and data, identifying and patching vulnerabilities in a timely manner, implementing malware protection, using principles of least privileges, restricting administrative privileges on all systems, regular backup of systems and data to offsite locations, and creating incident response plans with clear procedures on how to respond in the case of a ransomware attack. Carefully plan, implement, and regularly test your data backup and restoration strategy. It's important not only to have secure backups of all your important data, but also to make sure that backups are kept isolated so ransomware can't readily spread to them.

There are many resources and recommendations available to help organisations in these efforts. The best-practices outlined in this document and the best-practices for maritime organisations and vessels cover the steps needed in order to protect against ransomware attacks. By implementing the best-practices in the organisation's cybersecurity approach, the risk of ransomware can be minimised and the organisation's operations kept running.

Some information regarding the Emotet ransomware is included in chapter 6.5. NCSC-FI Reported incident statistics

Links to NCSC-FI cybersecurity breach and ransomware protection resources:

- *https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/guide-protecting-yourself-against-data-breaches*
- *https://www.kyberturvallisuuskeskus.fi/en/emotet-malware-actively-spread-finland*
- *https://www.kyberturvallisuuskeskus.fi/en/news/active-ransomware-attacks-continue*
- *https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf*

Links to NIST guidance on ransomware protection and response:

- *https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks*
- *https://www.ncsc.gov.uk/blog-post/what-board-members-should-know-about-ransomware*
- *https://www.ncsc.gov.uk/blog-post/rise-of-ransomware*
- *https://csrc.nist.gov/projects/ransomware-protection-and-response*
- *https://csrc.nist.gov/CSRC/media/Publications/nistir/draft/documents/NIST.IR.8374-preliminary-draft.pdf*
- *https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Tips_for_Preparing_for_Ransomware_Attacks.pdf*

[20] https://go.druva.com/rs/307-ANG-704/images/Executive-Brief_2017-Druva-Annual-Ransomware-Report_WEB_Q118-CON-10765.pdf

4. BEST PRACTICES FOR MARITIME CYBERSECURITY

Due to the IMO Cyber Risk Management requirements, many guidelines have been published by maritime sector organizations and associations to help organisations meet the new requirements and to improve the cybersecurity onboard vessels. It is highly recommended that all maritime operators familiarise themselves with these documents and guidelines to get an understanding of maritime cybersecurity and to improve cybersecurity in their environments.

These guidelines, however, can be complex to understand and implement in complex maritime environments. Maritime operators and seafarers want clear, concise and practical instructions and checklists that can be easily understood and implemented onboard vessels. These best practices have been created so that maritime operators can get a good start with improving their cybersecurity posture and take the necessary steps to be in line with the IMO cybersecurity risk management requirements.

4.1. Best practices

The best practices consist of the following steps/areas:

1. Senior Management Support
2. Cybersecurity awareness training
3. Cybersecurity procedures, guidelines and instructions
4. Critical services and functions in the organisation
5. Cybersecurity risks assessment
6. Risk management plan
7. Cybersecurity governance and architecture
8. Supply chain cybersecurity
9. Incident management, response and recovery
10. Cybersecyrity standards and frameworks
11. Collaborate with external parties

These best practices are a list of necessary actions to be done in order to be compliant with IMO requirements combined with more comprehensive security governance actions that are needed to manage cybersecurity.

4.1.1. Senior management support

Organisations are becoming increasingly dependent on digital services and systems while facing an increasing amount of cyber threats. Cybersecurity is a top level, cross-functional issue that affects the whole organisation. The risk of cyberattacks span over business functions and departments, suppliers, and customers. There are challenging decisions that have to be made in becoming more cyber resilient, decisions that are necessary and can only be achieved through active participation from the CEO and senior management members. The senior management key mission is to support activities that benefit the organisation. This is why senior management must have a basic understanding of cybersecurity and associated risks to the organisation.

Cybersecurity has previously not been a high priority on the senior management agenda and has been seen as a responsibility of the IT department alone.

However, this is changing and senior management is getting more aware of the cyber threats and risks and their potentially devastating effects on the business. To successfully design, plan and implement a cybersecurity strategy that complies with maritime regulations and business requirements, the organisation has to continuously invest in cybersecurity. It is not sufficient to just buy a piece of equipment to implement cybersecurity.

The continuous investment will include resources like dedicated cybersecurity personnel, security governance, processes and technologies. This will require allocation of budget and resources and this needs to be approved and supported by senior management. Without senior management support, the cybersecurity efforts will most likely fail.

Cybersecurity and cyber risk management requires continuous engagement of the company's senior management , instead of just involving the ship security officer or the IT manager:

- The potential effect of cybersecurity risks can have a destructive potential on the safety of the crew and vessel as well as the performance and reputation of the company.

- Cybersecurity risks are not only IT issues but risks that may severely impact the performance and the reputation of the company.

- Implementing cybersecurity in a company will most likely affect business procedures and operations and require more time and resources. It is therefore important to get senior management support and insight into cybersecurity decisions and mitigations to ensure all risks and actions are aligned with the business risk management strategy

- Cybersecurity initiatives may change how the business operates and how the company interacts with customers, authorities, and suppliers and create new requirements on how these interactions are done. It is a senior management responsibility to decide how these changes will be implemented so that they support the established business strategy and objectives.

To get senior management support, it will be crucial to increase the understanding of threats and risks to the business and what the consequences are if such threats and risks would materialize. Risk management is something that senior management is used to and talking about cybersecurity using risks and their impacts on the business is the best way to get understanding and support.

The following areas are key to engaging senior management in cybersecurity:

- **Include cybersecurity risk on the senior management agenda**. Just as with other enterprise risks, CEOs and senior management must provide input on the organisation's risk appetite for cybersecurity related risk including loss of intellectual property, disclosure of customer information and disruption of business operations. This is specifically important with risks that affect the safety of vessels and crew. The different departments of the organisation must help with identifying and prioritizing risks and make trade-offs between risk reduction and operational impact and safety. The organisations cybersecurity managers or persons responsible for cybersecurity should engage with senior management and discuss cybersecurity from a risk perspective and get them engaged in cybersecurity decisions using cybersecurity risk management as a tool for effective decision making. Start small and present the identified cybersecurity risks, their probabilities and impacts to the business together with an action plan on how to mitigate or minimise the risks. The senior management decisions regarding cybersecurity efforts will be much easier and effective with using risks as a starting point.

- **Engage cybersecurity across all business functions and departments**. Senior management must ensure that cybersecurity is incorporated into all areas of the business, from IT operations to maritime operations, supply chain management and human resource. Cybersecurity must be prioritised and senior management plays a crucial role in setting a good example for the rest of the organisation.

- **Supporting changes in human behaviour and culture**. Cybersecurity is not an IT issue but rather an company wide issue that affects everyone, from senior management to employees and crew. It is therefore important that senior management is actively involved in and supports cybersecurity initiatives and shows good examples to the rest of the organisation. If senior management takes cybersecurity seriously, so will the employees.

- **Ensuring cybersecurity governance and reporting**. No matter how clear and pragmatic cybersecurity policies, procedures and controls are, some individuals will try to circumvent them to do their jobs. It might be because of not understanding the risks, project time constraints, deadlines or budgets. Senior management needs to make sure that policies, procedures and controls make sense from a business standpoint and ensure that they are followed by the organisation. Additionally, senior management should create effective reporting on how the organisation is progressing with established cybersecurity programs and continuously evaluate decisions and actions to ensure that the program is effective.

4.1.2. Cybersecurity awareness training

Training and cybersecurity awareness is crucial to the whole organisation. Employee support and understanding are key to any successful project. Ensure that your employees, from senior management to crew, know what cybersecurity means and what they can do to ensure that your environment is kept secure. This can be done by cyber-security awareness efforts, training, courses and webinars, as well as internal communications from those responsible for cybersecurity in your organisation. It is important that all employees, including management, receive training to get a better understanding of cybersecurity and what it means to the organisation.

4.1.3. Cybersecurity procedures and instructions

The vessel crew needs to have clear and concise procedures that define how they should manage cybersecurity on the vessel. The following procedures should be considered and created:

- Procedures for how to use onboard systems and services
- Procedures on how to manage external media
- Procedures on how to update and manage vessel systems
- Procedures on how to use personal devices, crew networks and Internet
- Procedures for supplier remote access
- Procedures for cybersecurity incident management
- Procedures for cybersecurity exercises

These procedures should describe the essential requirements and activities that the crew needs to be aware of in their daily operations.

4.1.4. Critical services and functions

The first step in any maritime cybersecurity activity is to identify the critical services and functions and their related IT- and OT-assets used in the organisation and on the vessels. To address cybersecurity you first have to know what you have. The best way to do so is to create an asset inventory for all assets that are used in the organisation and specifically on the vessels. The asset inventory should contain all assets that are critical to the organisation and are needed to support and deliver the functions and services that the business provides. This includes physical assets, devices, systems, software and applications for both IT and OT.

The asset inventory process can be created in several ways, from manually documenting assets in spreadsheets to using automated tools to identify and classify connected assets over the network. Usually, a maritime organisation has some systems to manage the operational maritime assets on vessels but these systems are not normally used for IT and OT assets that are critical to the cybersecurity of the organisation.

Before any risk assessments can be planned and conducted, the asset inventory needs to be completed. There are many different models and spreadsheets publicly available that can be used to get started, and we recommend starting with DCSAs "*Asset Management and Risk Register Templates Reading Guide*"[21] that includes usable templates for asset inventories and risk management:

4.1.5. Risk assessment

After the asset identification and documentation, a risk assessment should be made to identify threats, risks and vulnerabilities related to the assets that can negatively impact the operations and safety.

All identified risks must be assessed and corrective actions identified, documented and implemented to manage the risks. The risk management process can be done in several ways but typically this means documenting risks in spreadsheets. Other risk management tools are available but can be expensive and the easiest way to get started is by using existing risk assessment spreadsheets. When the risk management practices become mature, it is worth investigating other tools to support the risk management process as working with spreadsheets can become tedious and time-consuming.

There are many different models and spreadsheets publicly available that can be used to get started, and we recommend starting with DCSAs "*Asset Management and Risk Register Templates Reading Guide*"[22] that includes usable templates for asset inventories and risk management.

RISK EXAMPLE

Risk of malware infecting vessel systems

Risk probability: HIGH

Risk impact: HIGH

Risk consequence impact: 1-1.5MEUR

Risk remediation cost: 150kEUR/year

Risk description: *Risk of malware, specifically ransomware, infecting our vessel computers and disrupting operations and affecting vessel safety, ability to sail or disembark cargo in port. The probability for the risk is high and the impact is high. The monetary impact is considerable, amounting to 1-1.5MEUR..*

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

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

4.1.6. Risk management plan

When 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 in order to minimise and remediate risks.

The action plan should be documented with responsible persons, timeplans and resources needed for each task. The implementation of actions requires senior management approval and support based on the identified risks and their potential impact to business operations.

4.1.7. Cybersecurity architecture

Based on the assets, risks and remediations that have been identified, a cybersecurity architecture should be developed and documented in order to ensure that the ISPS requirements for a Ship Security Plan (SSP) are followed and that the SSP contains cybersecurity elements. This includes measures taken to address identified risks, cybersecurity responsibilities of the crew, procedures for responding to cybersecurity threats, procedures for auditing cybersecurity activities. All these cybersecurity activities can not be performed by the crew alone and has to include provisions for collaborating with the organisation's officers and teams responsible for cybersecurity. The cybersecurity elements can be documented in a separate Ship Cybersecurity Plan (CSP) if needed, as the SSP typically focuses heavily on physical security. As cybersecurity is a continuously evolving area, it is recommended that the maritime operator considers the practical impacts of frequently updating and distributing the plans to the vessels.

The overall contents for the CSP can be derived from the ISM/ISPS Chapter 9: Ship Security Plan[23] but with a focus on cybersecurity:

> *9.4 Such a plan shall be developed, taking into account the guidance given in part B of this Code, and shall be written in the working language or languages of the ship. If the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included.*

Traditional SSP documents will rarely include cybersecurity policies, controls or procedures. It is recommended[24] that this is documented in the separate CSP and include information, references and procedures such as:

- Risk analysis of information technology IT systems
- Preventive security measures deployed in the ship and ashore to mitigate risks in IT systems to an acceptable level.
- Internet access security policy indicating restrictions applicable depending on the operations being performed on the ship.

[23] https://www.classnk.or.jp/hp/pdf/activities/statutory/isps/code/ISPS_CodeA.pdf
[24] https://erawat.es/en/incorporating-maritime-cybersecurity-in-isps-and-ism

- Policy for the use of removable storage media such as usb sticks, external drives, CDs and DVDs.
- Policy and network access controls for the crew and wireless WiFi networks.
- Policy and procedures for updating and maintaining information and navigation systems.
- Physical and logical access controls to the various ship systems based on its sensitivity level.
- Authorization criteria for remote connections from the company office for system monitoring and maintenance.
- Contingency plan for information technology IT systems.
- Cyberincident management procedures: detection, reporting, assessment and decision, response, recovery and lessons learned.
- Training and awareness of master, officers, engineers and crew on cybersecurity risks and controls.

4.1.8. Supply chain cybersecurity

The maritime sector is highly dependent on various external suppliers and 3rd 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, etc.

Cybersecurity is said to be as strong as the weakest link, and any security incidents in the supply chain may have devastating consequences for the maritime operator. Therefore it is important to assess the cybersecurity of the supply chain suppliers to identify risks in their services and systems that can negatively impact the operation of the vessels.

Maritime operators must continuously manage their suppliers and their cybersecurity to minimise risks caused by the supplier. The suppliers may have remote access to critical systems onboard, and any cybersecurity incident on the supplier side could affect the vessels and the systems they are responsible for.

The suppliers should be subjected to cybersecurity requirements that ensure that their systems and processes are managed according to good cybersecurity practices. These requirements should be included in maintenance agreements with the suppliers.

Supply chain security management includes assessing the supplier regarding their cybersecurity and performing a risk assessment and documenting and establishing cybersecurity requirements for the supplier and ensuring that they follow these requirements.

- Perform supplier risk assessment
- Create supplier cybersecurity requirements
- Include cybersecurity requirements in supplier agreements
- Ensure the right to audit is included in supplier agreements

By performing these activities you can control and manage the cybersecurity of your suppliers by knowing the risks, establishing appropriate requirements, implementing controls and regularly assessing that the supplier meets established requirements and agreements.

Good and actionable guidance on supply chain security can be found in UK NCSC Supply chain security guidance[25].

4.1.9. Incident management, response and recovery

Effective incident management enables maritime operators to quickly identify cybersecurity incidents and to quickly respond and recover from the incident so that the impact of the incident does not affect the safety of the vessel.

Maritime operators should implement necessary policies, procedures and controls that enable them to detect, respond, recover, learn and improve from cybersecurity incidents. This includes both procedural and technical measures, such as, documenting vessel cybersecurity incident response plans and procedures, implementing logging and monitoring, and training the crew in how to detect and respond to cybersecurity incidents.

It is also important to regularly train the crew in incident management by doing cyber exercises. NCSC-FI has published guidelines for organising cyber exercises:

- *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 employees in the crew to respond to cyber incidents.

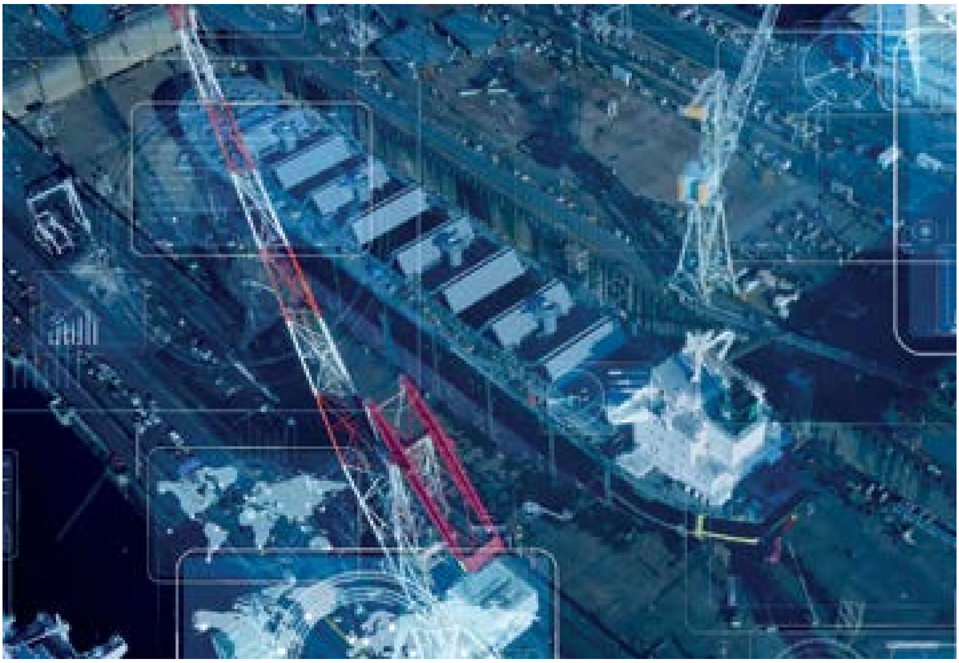
4.1.10. Cybersecurity standards and frameworks

Cybersecurity is a complex field, from top-level policies, processes and procedures down to technical details and the configuration of devices in the environment. The practice of managing, controlling and directing cybersecurity in an organisation is called cybersecurity governance. Security governance includes all aspects of cybersecurity, from policies, processes and procedures to technical controls and employee awareness.

Well implemented security governance will effectively coordinate the cybersecurity activities of your organisation. It enables the flow of cybersecurity information and decisions around your organisation.

It can be very challenging to manage all aspects of cybersecurity governance without using help and guidance from existing standards and guidelines. There are many existing frameworks and standards that can be used to create an effective cybersecurity governance framework.

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



Furthermore, since the publication of the IMO resolution MSC.428(98) in 2017, many maritime specific guidelines have been published by various organisations in the maritime sector. Below is a list of guidelines commonly used and developed for the maritime sector:

- BIMCO Guidelines on Cyber Security Onboard Ships[26]
- DCSA Cyber Security Guide[27]
- UK Code of Practice: Cybersecurity for ships[28]
- DNV-GL-RP-0496: Cybersecurity resilience management for ships and mobile offshore units in operation[29]
- DNV-GL-CP-0231: Cyber security capabilities of control system components[30]
- IACS Recommendation on Cyber Resilience[31]

These guidelines commonly reference the following standards:

- ISO 27001
- ISA/IEC 62443 Industrial Control System Security
- NIST Cybersecurity Framework (NIST CSF)[32]

26) https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx

28) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf

29) https://brandcentral.dnvgl.com/download/DownloadGateway.dll?h=BE1B38BB718539CC0AB58A5FF2EA7A83DE6D49BC96B8DB13C4CAAFA95E9ACCDA9F12593F5BB9D3D16F4B2EB2FF9780D9

30) https://rules.dnv.com/docs/pdf/DNV/CP/2018-01/DNVGL-CP-0231.pdf

32) https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework

The ISO 27001 standard is usually mentioned as an option for creating an information security management system (ISMS) for managing cybersecurity in the organisation.

Due to the nature of the maritime environment, which has to manage a wide variety of technologies, including IT and OT systems, the ISO 27001 standard is not fully aligned with the maritime environment requirements. The maritime operating environment is similar to industrial control systems, where the OT systems control and affect physical systems and devices such as vessel navigation, engines and power systems, ballast tanks, cranes, cargo and other physical systems that control various functions of the vessels.

Standards like 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.

The NIST CSF is mentioned in many of the maritime guidelines and ISO/IEC 62443 has been extensively used by DNV-GL in their cybersecurity guidelines and publications. Therefore it is worth looking into these standards when developing a cybersecurity program for the maritime environment. The ISA/IEC 62443 standard goes into detail on how cybersecurity should be managed in industrial control networks, outlining different security zones and network segmentation for different functions.

4.2. 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. There have been many cybersecurity guidelines and information published for the maritime sector from various sources, both public and private, that can be used. In the area of cybersecurity, it is also important for maritime operators to collaborate and share information, experiences and good practices and get external help if deemed necessary.

It is highly recommended that the maritime sector use these resources and collaborate in order to improve the cybersecurity in the secor as a whole.

5. SURVEY RESULTS

As part of the project initiated by the Finnish Shipowners association together with the National Emergency Supply Agency in Finland an online survey was conducted among the members of the Finnish Shipowners Association. The survey content was based on the National Cybersecurity Centre Cybermeter Assessment Tool (see 7. APPENDIX B: CYBERMETER MATURITY LEVELS), a national framework for the assessment of cybersecurity capabilities (Kybermittari arviointityökalu) including some details and refinements towards the maritime industry. The purpose for the online survey was to get insights into the Finnish fleet maritime cybersecurity maturity.

The survey was conducted in two parts:

- **Organisational survey**, focusing on how cybersecurity is managed in the organisation, including the vessels
- **Vessel survey**, with focus on the technologies used on the vessels and how the cybersecurity of IT and OT assets are managed, operated and updated

The survey was then followed up by in-depth interviews together with a subset of the respondents to get more valuable and accurate information from the survey results and ensure the data and answers are aligned with reality. The survey was sent to 25 Finnish Shipowners Association members of which 6 responded to the organisational survey and 38 vessels responded to the vessel survey.

In the survey, the majority of respondents (83%) reported their overall cybersecurity is good or excellent. 67% of respondents report their GDPR compliance as good. Half of the respondents (50%) reported that the status of the IMO resolution 428 (98) regarding cyber risk management is good and the other half said the status is fair. Half of the respondents (50%) were unaware of the effects and requirements of the EU NIS directive on maritime operators.

The survey data shows that the cybersecurity maturity level for the Finnish maritime sector is relatively low with an average **Maturity level 1 (MIL-1)** between all respondents. Maturity Level 1 is described as follows:

> **MIL-1:** *Initial practices are performed but may be ad hoc*

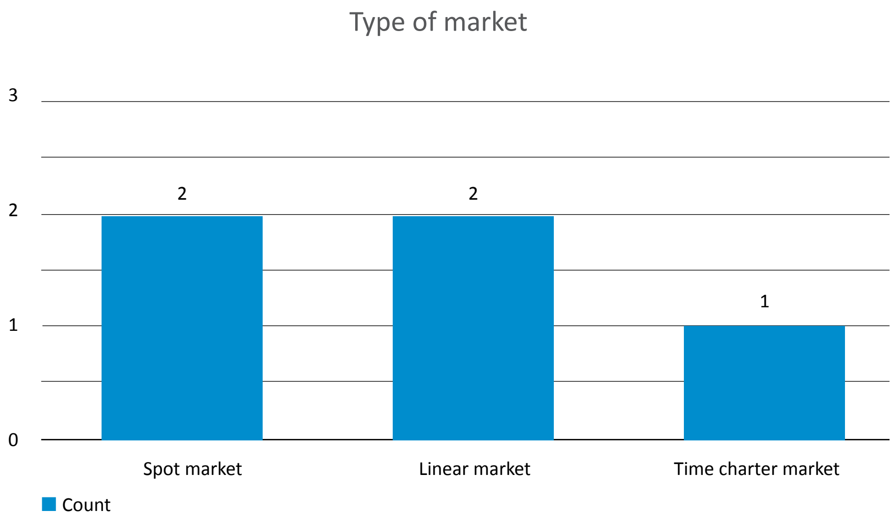
Due to this maturity level and with cybercriminals continuously becoming more sophisticated in their attacks, it is inevitable that cyberattacks against maritime operators and vessels are becoming the norm rather than the exception. The Finnish maritime operators need to improve their cybersecurity to ensure that their organisation, fleet and vessels are sufficiently protected and resilient against the increasingly sophisticated cyber threats.

5.1. Organisational survey

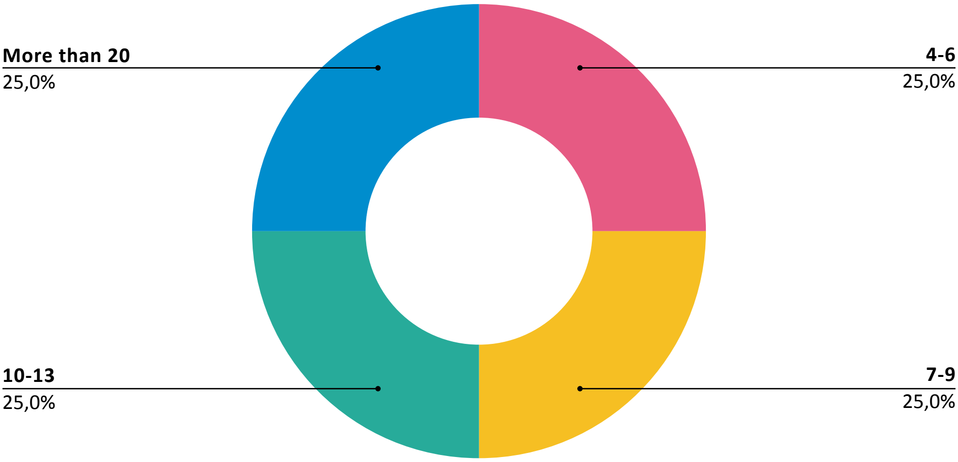
The organisational survey was distributed to all members of the Finnish shipowners association. The purpose of the organisation survey was to measure how cybersecurity is managed in the organisation, including the vessels.

Survey participants information

The types of markets for the survey participants consist of spot market, liner market and time charter market operators.



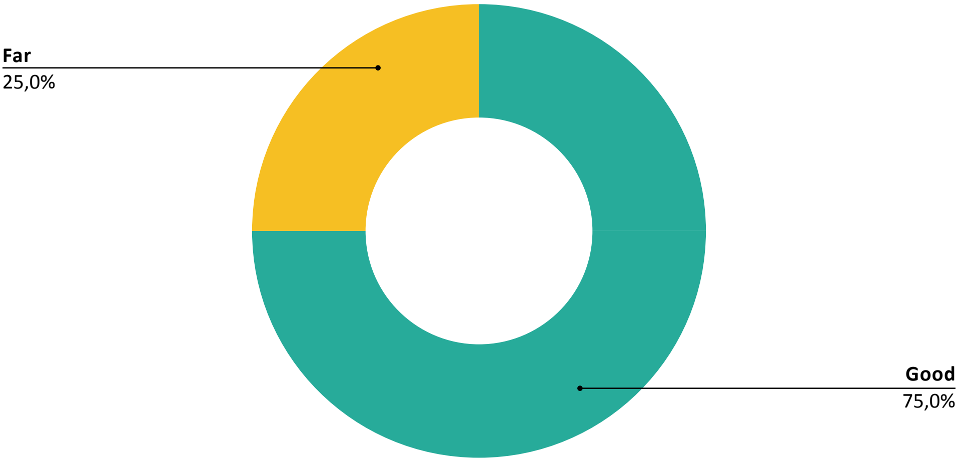
Organisation fleet size



The respondents organisation fleet size in number of vessels can be seen in the chart above, with a dispersion from 4-6 vessels to more than 20 vessels in the fleet. 75% of the organisations have a fleet of 4-13 vessels.

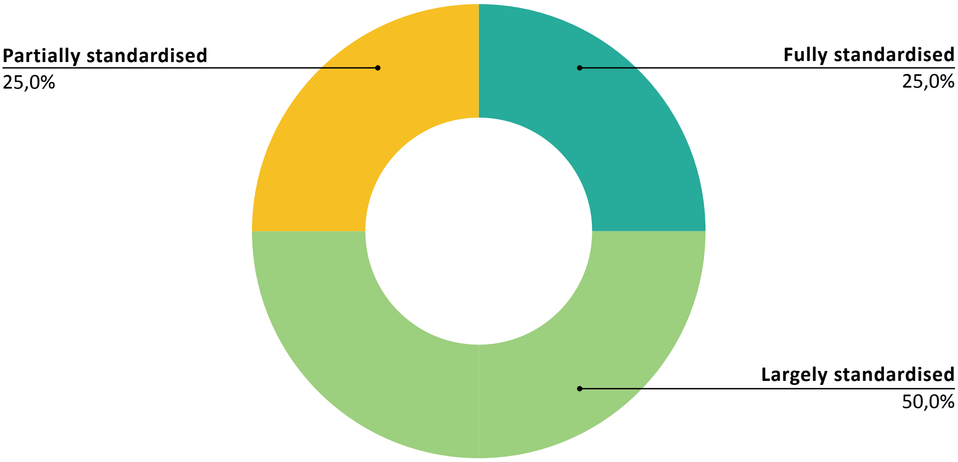
Overall status of cybersecurity

What is the current status of cybersecurity in the organisation?



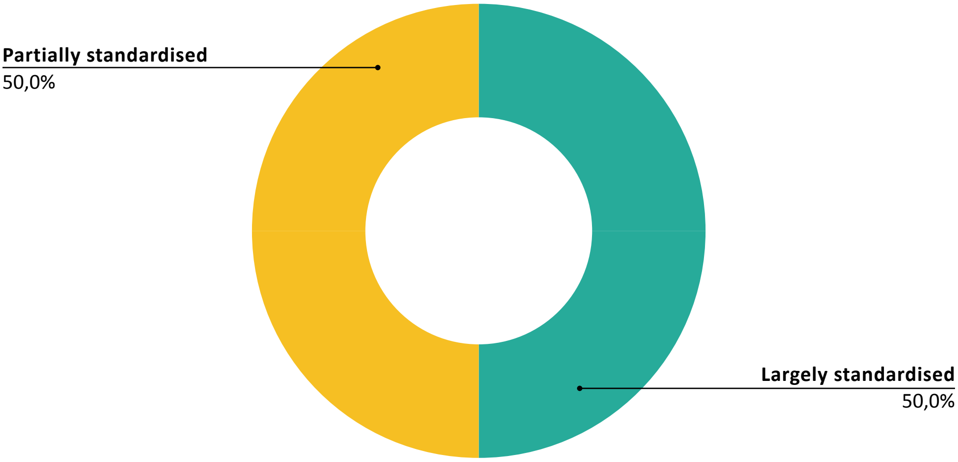
The respondents' self assessment of the overall status of cybersecurity in the organisations is deemed to be good based on the survey results, according to 75% of respondents. 25% reported their status to be fair.

Maritime information technology (IT) standardisation across the fleet



The information technology (IT) standardisation level across respondents fleet is largely (50%) standardised according to the results. 25% report that their IT in the fleet is fully standardised and 25% report that it is only partially standardised.

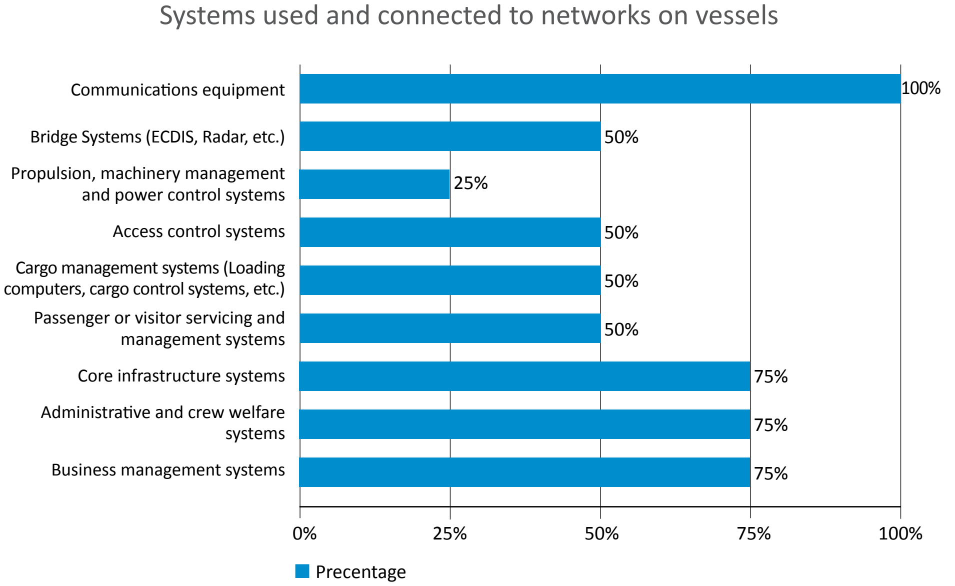
Maritime operations technology (OT) standardisation across the fleet



The operational technology(OT) standardisation level is lower than the IT environments, with 50% largely standardised and 50% partially standardised.

Vessel systems

According to the respondent data, the vessels are typically equipped with various kinds of of IT and OT systems that are connected to the networks. More specific details on network connectivity for the different systems can be found in the vessel survey chapter, 5.2.2. Vessel systems

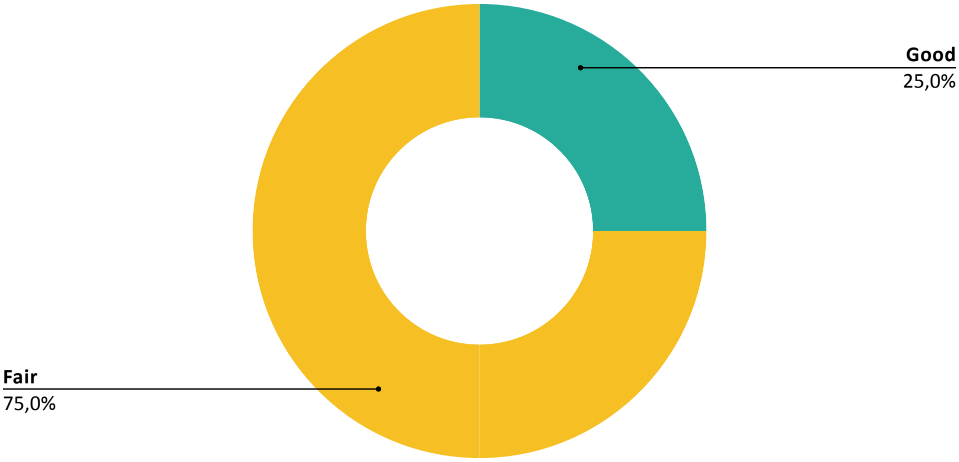

Systems used and connected to networks on vessels
Communications equipment
100%
Bridge Systems (ECDIS, Radar, etc.)
50%
Propulsion, machinery management and power control systems
25%
Access control systems
50%
Cargo management systems (Loading computers, cargo control systems, etc.)
50%
Passenger or visitor servicing and management systems
50%
Core infrastructure systems
75%
Administrative and crew welfare systems
75%
Business management systems
75%
0%
25%
50%
75%
100%
Precentage

The communication systems are naturally connected to vessel neworks. 50% of bridge systems, containing critical systems like ECDIS, AIS, GPS, Radar, are connected to vessel networks. Only 25% of propulsion, machinery and power management systems are connected to networks according to organisation respondents. 75% of core infrastructure, administrative and business management systems.

Cybersecurity usually uses a layered approach to protection measures, with multiple layers of security to protect assets. A layered approach increases the cybersecurity of the environment and minimises the potential effect of cybersecurity incidents affecting one layer of the protection. The data shows that some improvements can be made to the environment by adding layers of cybersecurity to the critical systems on vessels. Firewalls should be used to protect the vessel networks and network segmentation implemented to protect different types of equipment from each other. Logging and monitoring should be implemented in order to detect cybersecurity incidents. Antimalware protection should be implemented on all systems where possible, and alternative protection considered for systems where antimalware protection is not possible. For example, for OT systems with uncommon operating systems or supplier managed equipment where the organisation is not able to apply its own protection technologies.

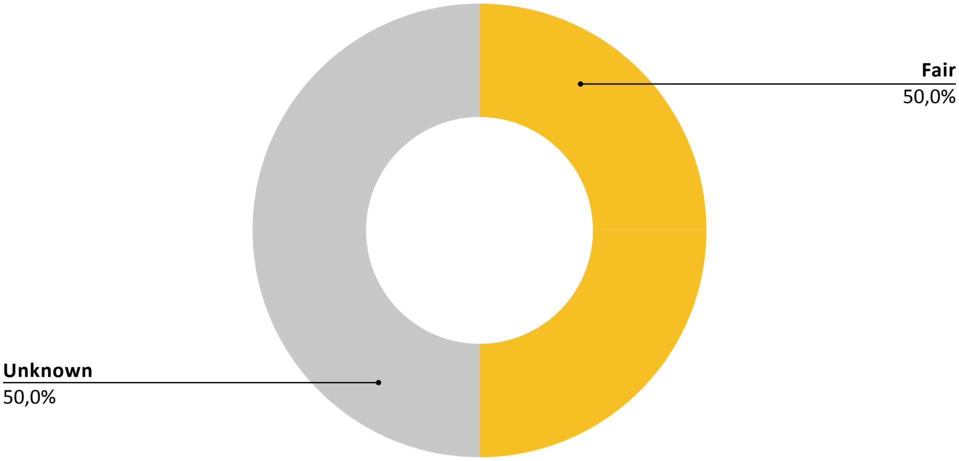
Cybersecurity in relation to IMO, NIS and GDPR

What is the current status of IMO cybersecurity resolution compliance in your organisation?



The respondents' self assessment on the overall status of IMO cybersecurity resolution preparedness in the organisations is deemed to be fair based on the survey results, according to 75% of respondents. 25% reported their status to be good.

What is the current status of NIS regulation compliance in your organisation?

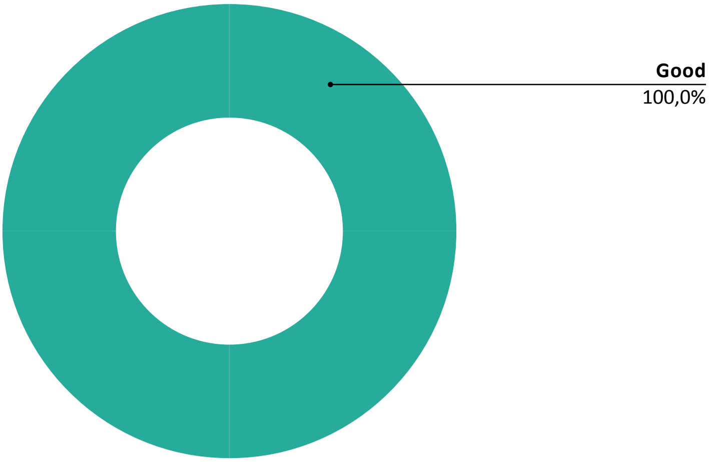


The NIS Directive[33] is an EU-wide legislation on cybersecurity. It focuses on the security of network and information systems and provides legal measures to boost the overall level of cybersecurity in the EU by ensuring Member States' cybersecurity preparedness. The directive focuses on sectors heavily reliant on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. The NIS directive is not mandatory for the Finnish maritime sector and the vessels but applicable to port operations.

33) https://digital-strategy.ec.europa.eu/en/policies/nis-directive

The overall status of NIS directive compliance in the organisations is deemed to be fair based on the survey results, according to 50% of respondents. 50% reported their status to be unknown. This shows that the maritime sector is not aware of the NIS directive.

What is the current status of GDPR regulation compliance in your organisation?



The respondents' self assessment on the overall status of GDPR regulation compliance in the organisations is deemed to be good based on the survey results, according to 100% of respondents. This is expected as GDPR has been mandatory since 25.5.2018.

5.1.1. Cybermeter Maturity Level

Based on the organisational survey data based on the Cybermeter model (More information see appendix B: 7. APPENDIX B: CYBERMETER MATURITY LEVELS) , the average cybersecurity maturity in the Finnish Maritime sector is deemed to be relatively low. The highest average maturity level for any of the control domains is Maturity Level (MIL-1) which is characterized by the following management practice:

> *Initial practices are performed but may be ad hoc. In the context of this model, ad hoc (i.e., an ad hoc practice) refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of organizational guidance in the form of a prescribed plan (verbal or written), policy, or training. The quality of the outcome may vary significantly depending on who performs the practice, when it is performed, and the context of the problem being addressed, the methods, tools, and techniques used, and the priority given a particular instance of the practice. With experienced and talented personnel, high-quality outcomes may be achieved even if practices are ad hoc. However, at this MIL, lessons learned are typically not captured at the organizational level, so approaches and outcomes are difficult to repeat or improve across the organization.*

The maturity levels are defined as follows:

- **Maturity Level 0(MIL-0):** Activities do not meet basic requirements.
- **Maturity Level 1(MIL-1):** Activities meet basic requirements, but mainly ad hoc, and the level of activities may vary from one situation to the next.
- **Maturity Level 2(MIL-2):** Activities are more advanced and comprehensive than at lower levels. In addition, the following describe the management of cybersecurity: Documented processes and practices; Sufficient resources and skills; and Defined roles and responsibilities.
- **Maturity Level 3(MIL-3):** Activities are advanced and comprehensive. In addition, the following describe the management of cybersecurity: Activities are steered by the organisation's policies (or similar guidelines); Performance goals have been set for activities, and they are monitored; and Documented processes and practices are in line with the organisation's standards, and their development is continuous.

A more detailed description of the maturity levels can be found in appendix A: 7. APPENDIX A: CYBERMETER MATURITY LEVELS

Compared to other sectors in the Finnish market, the Maritime sector maturity is LOW and there is reason to take action and improve cybersecurity in the organisations by implementing the best practices outlined in this report and the separate best-practices documents.

The Cybermeter model can be used to identify areas and actions that need to be improved to increase the cybersecurity maturity in the organisations.

5.1.2. Survey results per Cybermeter control area

The survey results have been combined and an average calculated for all answers from the participating organisations. Based on the collected data and the average response per each area and question, the maturity level for the Cybermeter domains/areas for the Finnish Maritime sector is as follows:

CSP – Critical Service Protection	**MIL 0**
RM – Risk Management	**MIL 1**
SCM – Supply Chain and External Dependencies Management	**MIL 1**
ACM – Asset, Change and Configuration Management	**MIL 0**
IAM – Identity and Access Management	**MIL 1**
TVM – Threat and Vulnerability Management	**MIL 1**
SA – Situational Awareness	**MIL 1**
IR – Event and Incident Response	**MIL 1**
WM – Workforce Management	**MIL 0**
CA – Cybersecurity Architecture	**MIL 0**
CPM – Cybersecurity Program Management	**MIL 0**

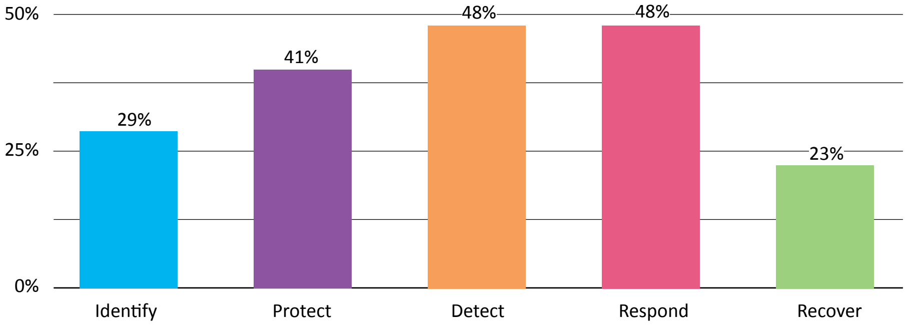
The following table shows the Cybermeter domains and and areas:

CSP – Critical Service Protection	MIL 0
Identification of Critical Services and their dependencies	MIL 1
Governance of Critical Services	MIL 1
Minimisation of the impact of cyber security incidents on Critical Services	MIL 0
RM – Risk Management	MIL 1
Manage Cybersecurity Risk	MIL 1
Establish Cybersecurity Risk Management Strategy	MIL 1
Management Activities	MIL 1
SCM – Supply Chain and External Dependencies Management	MIL 1
Identify Dependencies	MIL 1
Manage Dependency Risk	MIL 1
Management Activities	MIL 2
ACM – Asset, Change and Configuration Management	MIL 0
Manage IT and OT Asset Inventory	MIL 1
Manage Information Asset Inventory	MIL 1
Manage Asset Configuration	MIL 0
Manage Changes to Assets	MIL 1
Management Activities	MIL 1
IAM – Identity and Access Management	MIL 1
Establish and Maintain Identities	MIL 1
Control Access	MIL 2
Management Activities	MIL 2
TVM – Threat and Vulnerability Management	MIL 1
Identify and Respond to Threats	MIL 2
Reduce Cybersecurity Vulnerabilities	MIL 2
Management Activities	MIL 1
SA – Situational Awareness	MIL 1
Perform Logging	MIL 1
Perform Monitoring	MIL 1
Establish and Maintain Situational Awareness	MIL 2
Management Activities	MIL 1
IR – Event and Incident Response	MIL 1
Detect Cybersecurity Events	MIL 2

Analyze Cybersecurity Events and Declare Incidents	MIL 1
Respond to Cybersecurity Events and Incidents	MIL 1
Management Activities	MIL 2
WM – Workforce Management	**MIL 0**
Assign Cybersecurity Responsibilities	MIL 2
Develop Cybersecurity Workforce	MIL 1
Implement Workforce Controls	MIL 0
Increase Cybersecurity Awareness	MIL 0
Management Activities	MIL 1
CA – Cybersecurity Architecture	**MIL 0**
Establish and Maintain Cybersecurity Architecture Strategy and Program	MIL 1
Implement Segmentation as an Element of the Cybersecurity Architecture	MIL 2
Implement Application Security as an Element of the Cybersecurity Architecture	MIL 1
Implement Data Security as an Element of the Cybersecurity Architecture	MIL 0
Management Activities	MIL 1
CPM – Cybersecurity Program Management	**MIL 0**
Establish Cybersecurity Program Strategy	MIL 0
Sponsor Cybersecurity Program	MIL 0
Address Cybersecurity in Continuity of Operations	MIL 0
Management Activities	MIL 1

5.1.3. Survey results mapped to NIST CSF Functions

The survey results have been combined and an average calculated for all the answers to get an indication of the average cybersecurity maturity level in the maritime sector. The following graph and table shows the Cybermeter maturity levels mapped to the NIST Cybersecurity framework[34], showing the maturity status for each of the functions and associated controls, indicating how many of the NIST controls have been implemented in the organisation.



Identify	**29%**	Organization has a very limited capability to identify and manage cyber security risks to systems, people, assets, data and critical services. This typically leads to ineffectual resource and cost allocation and to failing to protect the critical services that the organization or external parties are dependent on. There is a rather high possibility of an unexpected cyber incident taking place that seriously impacts the core processes of the organization.
Protect	**41%**	Organization has a basic capability to protect its critical services from cyber security threats and incidents, but its coverage is not systematic, having several weak control areas. This typically means that the protection activities may not be targeted and scaled based on the criticality of service or information, leading on one hand to wasteful allocation of resources and money, and on the other hand to not protecting all critical services.
Detect	**48%**	Organization has a basic capability to collect data, but the ability to detect cyber incidents is hampered by the data quality and coverage and also by the analysis capability. Typically this means that response is delayed and the actions are not based on full understanding of the situation, leaving the organization exposed to major breaches and damage despite the initiated response.
Respond	**48%**	Organization has a basic capability to initiate a timely response to a cyber incident, but the process may not be well coordinated and rehearsed. Typically this means that even if the detection has been done early, it is still likely that the response is not able to contain the breach and damage.
Recover	**23%**	Organization has a very limited capability to initiate and execute recovery from the damage caused by a cyber incident. This typically means that the recovery will take unnecessarily long and therefore may significantly increase the brand damage, cost and impact of the incident.

[34] https://www.nist.gov/cyberframework

The maturity level of organisations can be improved according to the organization's readiness and will to invest in cybersecurity based on risk assessments, identified risks and required actions. The best practices outlined in this report is a good starting point to increase cybersecurity of the organisation and the vessels. NIST Cybersecurity framework can be used for identifying specific controls that can be implemented to raise the cybersecurity maturity in the organisation. An outline of the NIST Cybersecurity framework families and categories can be seen in the table below.

NIST Cybersecurity framework[35]

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset management	Access control	Anomalies and events	Response planning	Recovery planning
Business environment	Awareness and training	Security continuous monitoring	Communications	Improvements
Governance	Data security	Detection processes	Analysis	Communications
Risk management	Information protection processes and procedures		Mitigation	
Risk management strategy	Maintenance		Improvements	
	Protective technology			

5.2. Vessel survey

The vessel survey was distributed to all members of the Finnish shipowners association where the organisation was tasked to send out the survey to their vessels. The purpose of the vessel survey was to measure how cybersecurity is managed on the vessels and how critical IT and OT assets are managed, operated and updated with regards to cybersecurity.

The systems and technologies used on vessels vary depending on the age, size and purpose of the vessel. Bulk and Cargo vessels typically have less complex OT systems and technologies onboard compared to passenger vessels that have various IT systems and technologies in use to service their customers: Wireless networks, Sales systems, Payment terminals, etc.

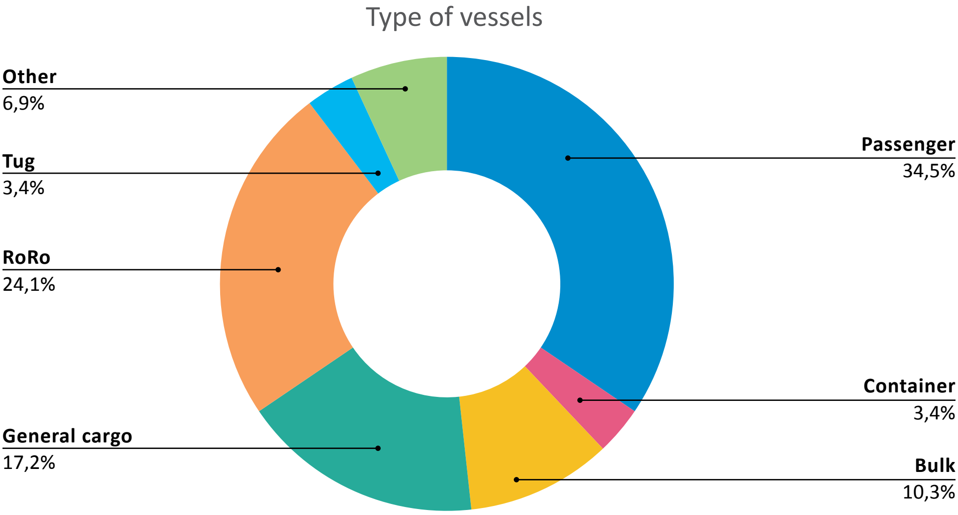
Operational systems like navigational systems, ballast systems, etc. are typically required and deployed on all vessels, but the systems vary depending on the age of the vessels. Newer vessels have modern systems that are typically connected to the vessel networks for monitoring and maintenance. Maintenance of critical operational systems are usually managed by the suppliers over remote connections.

[35] https://www.nist.gov/cyberframework

Some older systems are not network connected and the following diagram shows the types of systems typically used and connected to networks on vessels.

Type of vessels:

The type of vessels participating in the vessel survey were diverse, ranging from passenger vessels (34.5%), Roro (24.1%), General cargo (17.2%), Bulk (10.3%), Container (3.4%) and Tugs (3.4%). Other types reported were ropax and pusher/barge vessels.



Age of vessels:

The age of the vessels vary evenly, with newest vessels being 3 years and oldest 49 years. The average age of the vessels was 22.46 years.

Length of vessels:

The length of the vessels vary significantly, with the shortest vessels being 30 meters and the largest 220 meters. The average length of the vessels was 155.7 meters.

Vessel crew:

The size of the vessel crew varies from 3 to 190, with an average crew size of 36.11 persons. We can see from the crew size distribution that there is a cluster of crew sizes between crew size of 10-19 persons.

Vessel flag state:

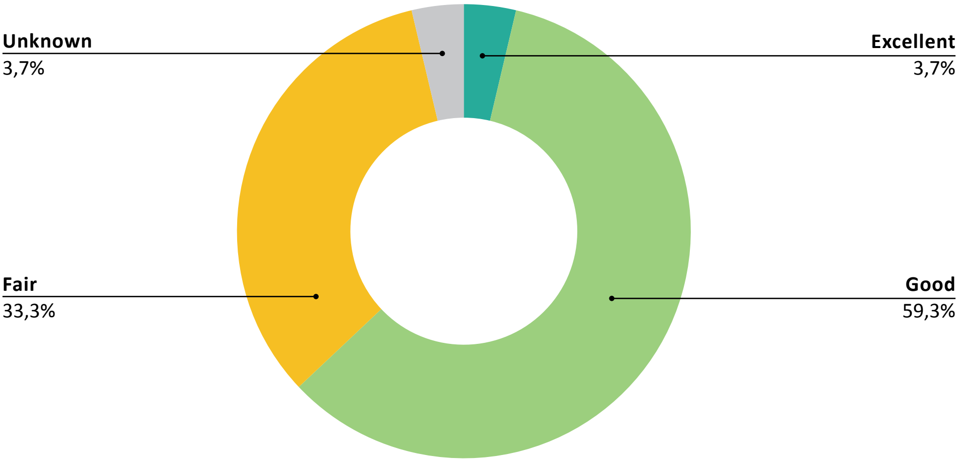
The flag state of the vessels in the survey is distributed between Finland, Sweden, Estonia and Åland.

5.2.1. Vessel cybersecurity status

Overall status of cybersecurity onboard vessels:

The respondents' self assessment of the overall status of cybersecurity on the vessels is deemed to be good based on the survey results, according to 59% of respondents. 33% considered their cybersecurity status to be fair. Only 3.7% report their vessel cybersecurity status to be excellent and another 3.7% stated that their cybersecurity status is unknown.

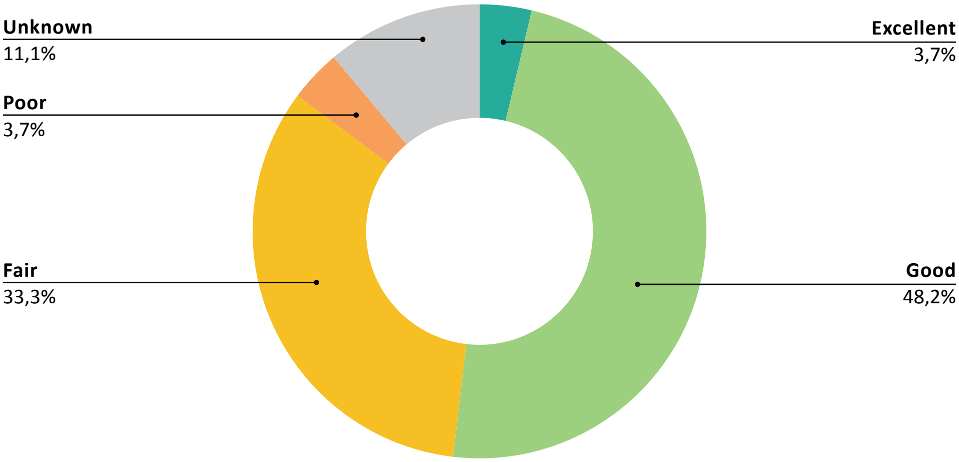
Current state of overall vessel cybersecurity



Overall status of IMO cybersecurity resolution compliance onboard vessels:

The IMO resolution MSC.428 (98) on maritime cyber risk management in safety management systems is in good standing according to 48.15% of the respondents. Although this resolution has been widely reported on and mandatory since 1.1.2021, 11.11% of respondents are still unaware of the resolution and how it affects their vessel.

Current state of vessel IMO cybersecurity regulation compliance



Overall status of NIS directive compliance onboard vessels:

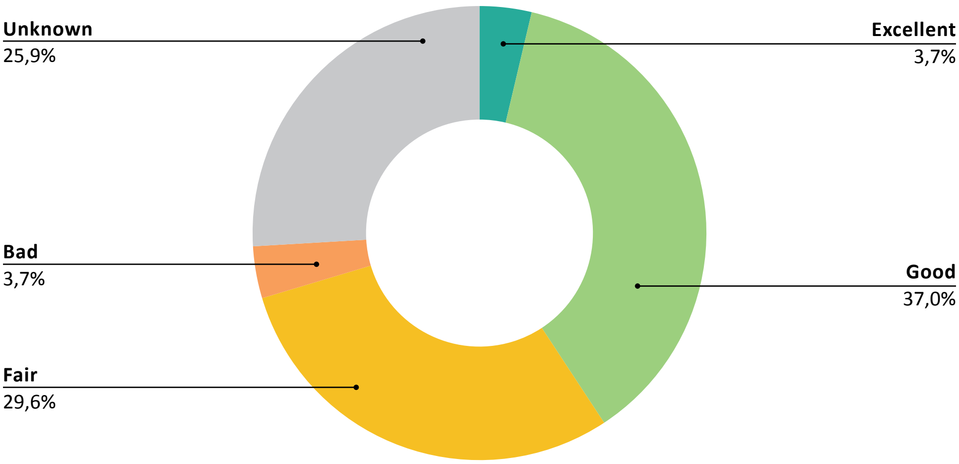
The EU NIS directive describes cybersecurity requirements for providers of critical services within the EU. Logistics and maritime operators are categorised as operators of critical services. ENISA[36] has reported that cybersecurity is getting more attention in the maritime sector, but has a relatively low awareness and focus compared with other sectors.

This can be seen in the survey answers where 37% respondents reported good and 29.6% reported fair preparedness. However, a total of 25.9% reported that the NIS directive is unknown and 3.7% reported that their NIS preparedness is bad.

The NIS directive is not mandatory for the Finnish maritime sector and the vessels but applicable to port operations.

[36] https://digital-strategy.ec.europa.eu/en/policies/nis-directive
https://safety4sea.com/cm-nis-directive-when-cyber-security-meets-operational-resilience
https://pwc.blogs.com/cyber_security_updates/2018/12/why-the-maritime-industry-must-get-on-board-with-the-nis-directive.html
https://static1.squarespace.com/static/57a8878837c58153c1897c2c/t/5c056515aa4a99ba1fb7f-2b1/1543857451926/14AthanasiosDrougkas_Athens18.pdf

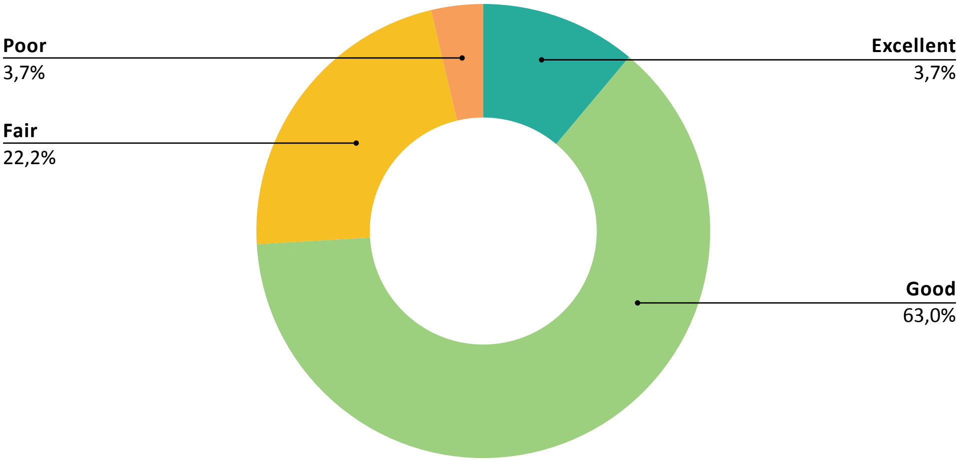
Current state of vessel NIS directive compliance



Overall status of GDPR compliance onboard vessels:

The EU General Data Protection Regulation (GDPR) came into effect 25.5.2018 and aims to protect the use of personal data. According to the survey, GDPR compliance is good for 63% of the respondents and only 3.7% reported poor compliance with the regulation.

Current status of vessel GDPR compliance



5.2.2. Vessel systems

The systems and technologies used on vessels vary depending on the age, size and purpose of the vessel. Bulk and Cargo vessels typically have less complex OT systems and technologies onboard compared to passenger vessels that have various IT systems and technologies in use to service their customers: Wireless networks, Sales systems, Payment terminals, etc.

Operational systems like navigational systems, ballast systems, etc. are typically required and deployed on all vessels, but the systems vary depending on the age of the vessels. Newer vessels have modern systems that are typically connected to the vessel networks for monitoring and maintenance. Maintenance of critical operational systems are usually managed by the suppliers over remote connections.

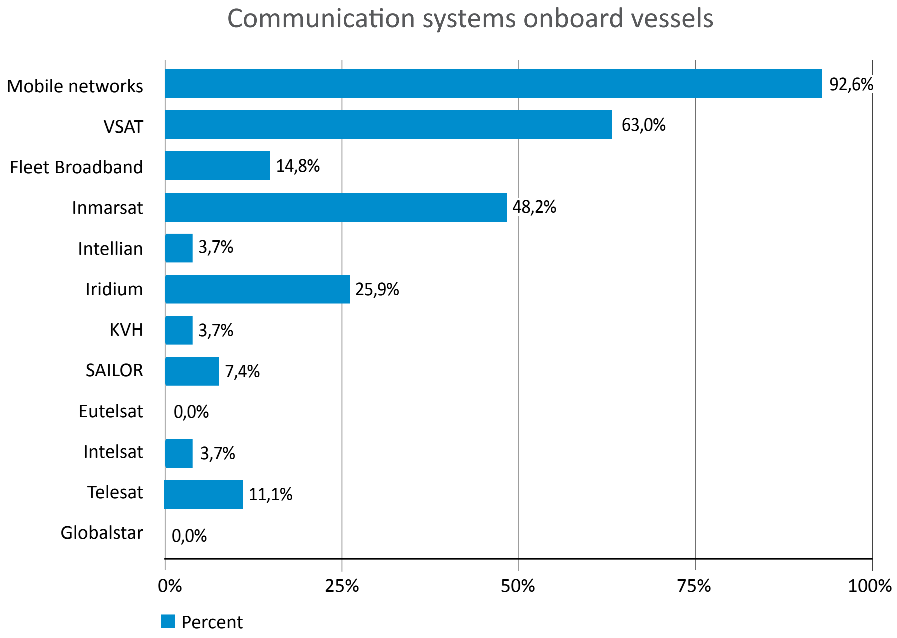
Some older systems are not network connected and the following diagram shows the types of systems typically used and connected to networks on vessels.

Age of systems

The average age of ECDIS systems on respondent vessels is 6.24 years and radar equipment is 12.27 years. The average age of all systems is 12.04 years.

Systems used on vessels

The vessels use a wide variety of communication systems, with mobile networks and satellite communication (VSAT) being the most common technologies used. Inmarsat (48%) and Iridium (26%) VSAT providers are the most commonly used.

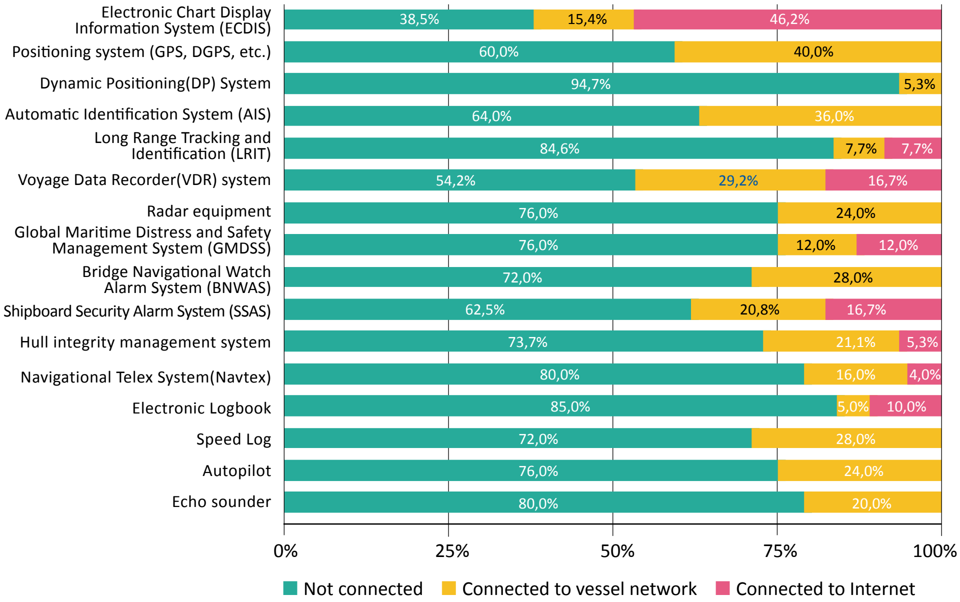


Systems connected to vessel networks

The diagrams below show how respondent vessel systems are connected to networks. The graphs are grouped by bridge systems, safety systems, cargo handling systems and administrative systems.

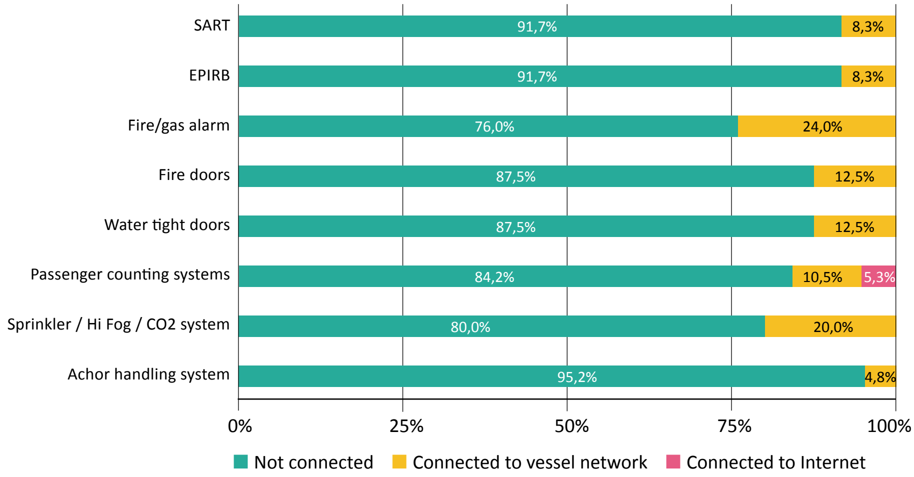
Many systems are still not connected to vessel networks on the majority of vessels, but systems are getting connected both to vessel networks and the Internet.

Bridge systems connected to vessel networks

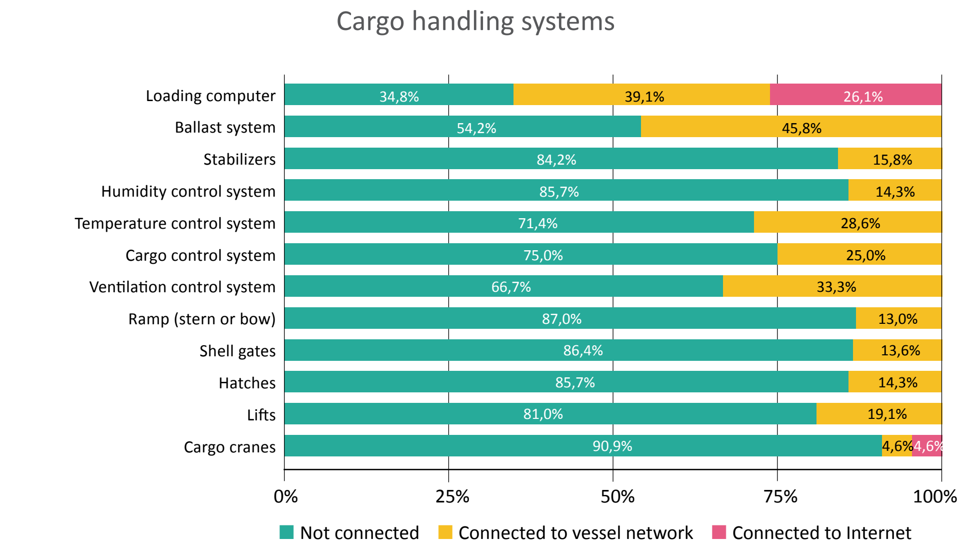


On the bridges, the most connected systems are ECDIS, VDR and positioning systems. A total of **46.2%** of respondent ECDIS systems are connected to the Internet, most likely due to receiving online updates to navigational charts.

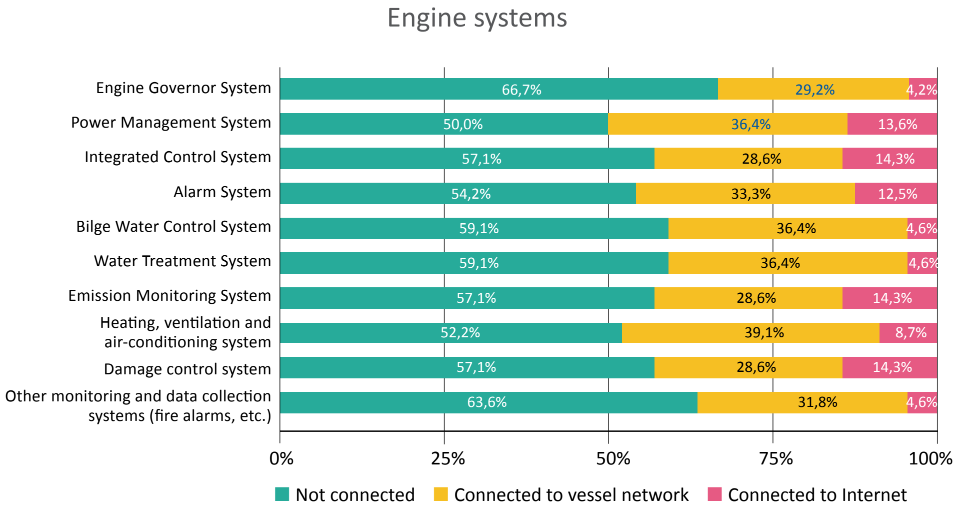
Safety equipment connected to the vessel networks



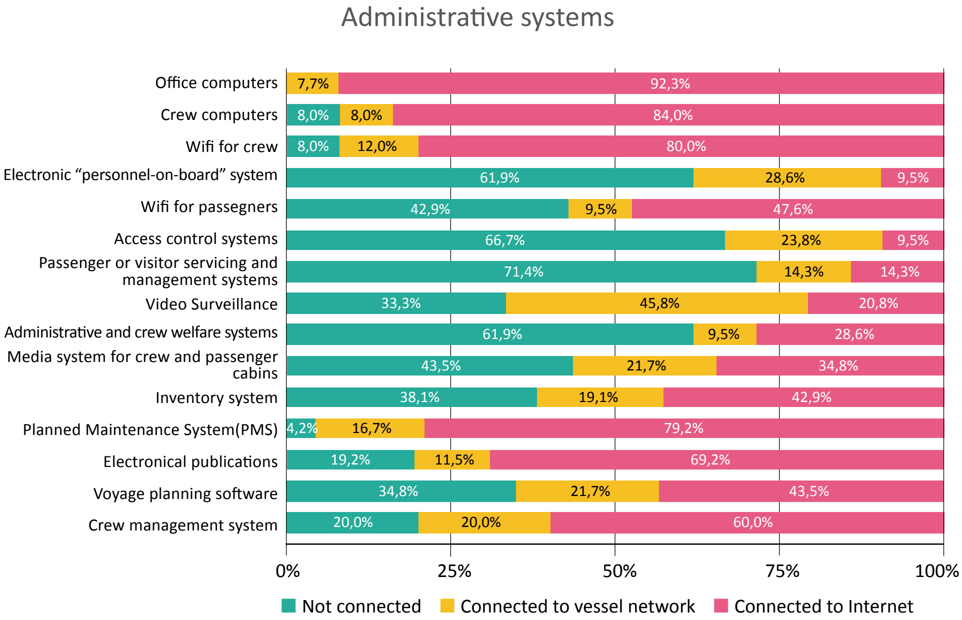
According to the respondent data, the safety systems are still quite unconnected to vessel networks. The most connected systems are fire/gas alarm systems with 24% of the respondents having them connected to vessel networks. Passenger counting systems are the only safety systems connected to the Internet with 5.3% of systems.


Cargo handling systems

For the cargo handling systems, the loading computers have the highest amount of Internet connections with 26.1%. The ballast systems have the highest amount of systems connected to vessel networks.


Engine systems

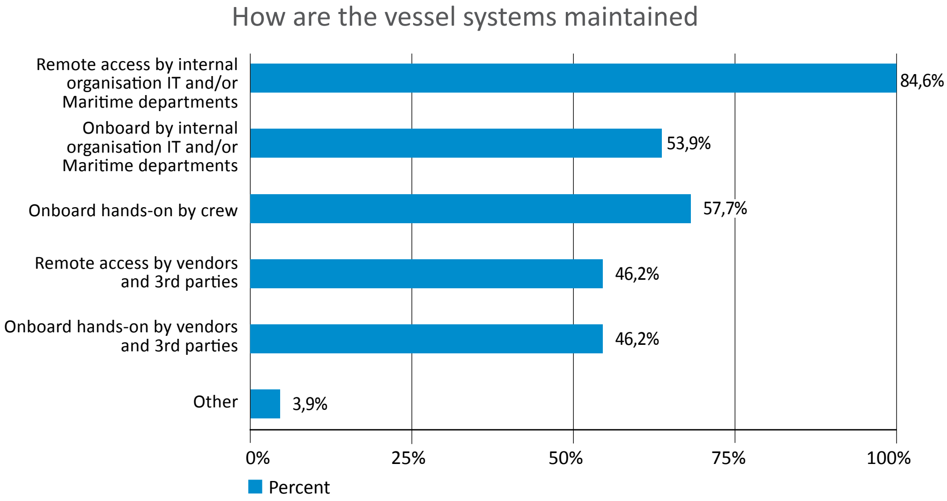
Engine systems have a high degree of systems connected to vessel networks and some also connected to the Internet. Power management, bilge water systems and water treatment systems systems have 36.4% connected to vessel networks. Integrated control systems and emission monitoring systems have the highest degree of Internet connections with 14.3% having access to the Internet. This is most likely due to these systems being operated by suppliers who need remote access to the systems. What is alarming with these results is that the engine systems are connected to vessel networks and to the Internet, which raises the risk for a cybersecurity incident. Proper network segmentation and access controls need to be implemented to protect these critical systems from cyberattacks.



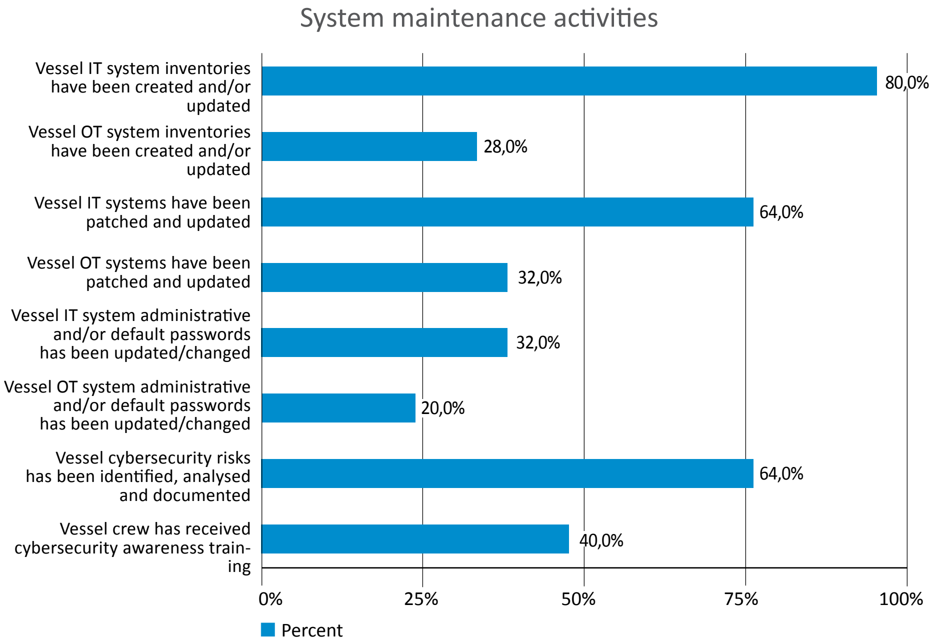
The administrative systems group has the most systems connected to vessel networks and to the Internet. This is quite natural since administrative systems are IT systems that usually require network connectivity to function, for example

In general, this data shows that vessel systems are getting connected to networks with an increased risk for cybersecurity related incidents. Special consideration and analysis should be made for critical systems like navigation and engine systems to ensure that these systems are properly segmented and controlled to minimise the risk of exposure to both vessel and external untrusted networks.

Maintenance and updates



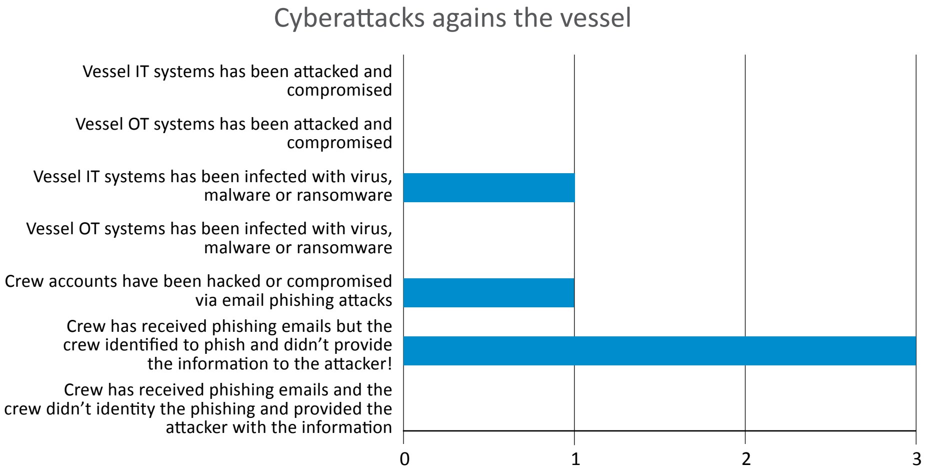
The data show that 86.4% of respondent vessels are maintained via remote access by the internal IT organisation or marine departments. This means that the systems maintained are connected to the vessel networks and hence susceptible to cyber attacks. 46.2% of systems are maintained by suppliers and other third-parties indicating the need for proper supplier cybersecurity management.



On 80% of vessels, the IT system inventories have been created and updated whereas only 28% of vessels have OT system inventories created and updated. Regarding updating systems, 64% of IT systems have been patched whereas only 32% of OT systems have been patched.

Default passwords have been changed for 32% of IT systems but only for 20% of vessel systems.
64% of vessels have conducted a cybersecurity risk analysis of vessel systems.
40% of the vessel crew has received cybersecurity awareness training.

One vessel reported that vessel IT systems have been infected with virus, malware or ransomware and one reported that crew accounts have been compromised via phishing attacks. Three vessels reported that the crew had received phishing emails but they identified the phishing attempt and did not provide any information to the attacker.



5.3. Summary of findings

According to the organisational survey, the cybersecurity maturity level of the finnish fleet is on average Maturity Level (MIL-1). There is room for improvement in all areas measured in the Cybermeter, (more information in):

CSP – Critical Service Protection	MIL 0
RM – Risk Management	MIL 1
SCM – Supply Chain and External Dependencies Management	MIL 1
ACM – Asset, Change and Configuration Management	MIL 0
IAM – Identity and Access Management	MIL 1
TVM – Threat and Vulnerability Management	MIL 1
SA – Situational Awareness	MIL 1
IR – Event and Incident Response	MIL 1
WM – Workforce Management	MIL 0
CA – Cybersecurity Architecture	MIL 0
CPM – Cybersecurity Program Management	MIL 0

Special focus is recommended in the **Maturity Level 0** areas with asset management, workforce management, cybersecurity architecture and cybersecurity program management(governance).

6. REFERENCES

- IMO MSC-FAL.1-Circ.3 Guidelines on Maritime Cyber Risk Management:

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

- IMO Resolution MSC.428 (98) Maritime Cyber Risk Management in Safety Management Systems

  https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

- BIMCO The Guidelines on Cybersecurity onboard Ships:

  https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

  https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx

- Digital Container Shipping Association Cyber Security Guide

  https://dcsa.org/standards/cyber-security-guide/

- NIST Cybersecurity Framework:

  https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework

- ISO 27001 *https://www.iso.org/isoiec-27001-information-security.html*

- ISA/IEC 62443 Industrial Automation and Control Systems Security

  https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

  https://www.isa.org/products/isa-62443-2-1-2009-security-for-industrial-automat

- DNV
  DNVGL-RP-0496 Cyber security resilience management for ships and mobile offshore units in operation:

  https://brandcentral.dnvgl.com/download/DownloadGateway.dll?h=BE1B38BB718539CC0AB58A5FF2EA7A83DE6D49BC96B8DB13C4CAAFA95E9ACCDA9F12593F5BB9D3D16F4B2EB2FF9780D9

  https://rules.dnv.com/docs/pdf/DNV/CP/2018-01/DNVGL-CP-0231.pdf

- UK NCSC Supply chain security guidance

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

7. APPENDIX A. FINNISH NATIONAL CYBER SECURITY CENTRE (NCSC-FI)

The Finnish National Cyber Security Centre (NCSC-FI, Kyberturvallisuuskeskus) is the central finnish authority for cybersecurity.

NCSC-FI provides services to finnish constituents in the areas of:

- Situation awareness and network management
- Monitoring and incident response
- Assessment, accreditation and guidance
- Exercises

The NCSC-FI Situation awareness and network management services provide valuable information to finnish organisations, such as

7.1. Situational awareness and network management

The situation awareness and collaboration management services of the NCSC-FI help to maintain and improve information security in our rapidly changing world.

NCSC-FI produces a variety of situation awareness products for organisations and citizens. Situation awareness products provide finnish organisations and citizens with up-to-date information about events and phenomena affecting cyber security. Services provided by NCSC-FI are listed below:

- Vulnerability reports
- Vulnerability digest
- Cyber weather
- Newsletter
- Information Security Now!
- Sector-specific situation awareness and notices
- Alerts
- Weekly report
- Annual information security review

7.2. Monitoring and incident response

NCSC-FI invites reports from private persons, businesses and organisations who suspect that they have fallen victim to an actual or attempted information security incident, such as malware infection, phishing or DoS attack.

Based on the reports, NCSC-FI can assist them in resolving and investigating the incidents and co-ordinating the required actions. NCSC-FI provides assistance to all Finnish actors within the limits of our available resources.

NCSC-FI helps with can, for example:

- share information
- contact collaborators and collaborative networks
- perform technical analysis
- provide legal guidance.

7.3. Assessment, accreditation and guidance

NCSC-FI's statutory obligation is to provide assessment and accreditation services. In addition, we provide information security guidance for governmental organisations and critical infrastructure providers.

NCSC-FI's duty to assess and accredit the security of information systems arises from the Act on International Information Security Obligations, Act on Background Checks and the Act on the Assessment of the Information Security of Public Authorities' Information Systems and Telecommunications Arrangements.

As for international classified data, NCSC-FI is the national Security Accreditation Authority (SAA), Crypto Approval Authority (CAA), National TEMPEST Authority, and Crypto Distribution Authority (CDA) (or National Distribution Authority, NDA), which is the authority responsible for the distribution of crypto material

The NCSC-FI provides information security guidance for governmental organisations and critical infrastructure providers. The aim is to prepare organisations for threats in the cyber domain and support clients in securing their operations and systems.

There are two types of information security guidance. One focuses on guidance related to protecting classified information. The other is guidance on more general cyber security issues in society.

7.4. Exercises

Cyber exercises aim at improving organisations' preparedness and response for severe security incidents, and at shortening and reducing the impact of cyber-attacks. An exercise involves presenting an organisation with a simulated crisis scenario to resolve, which enables the organisation to learn valuable lessons for developing its operations. The NCSC-FI supports critical infrastructure providers in their cyber exercise activities.

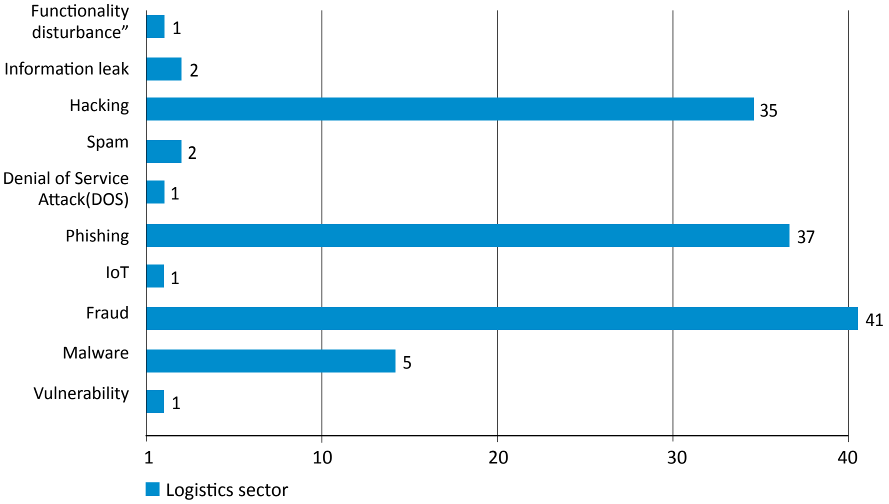
7.5. NCSC-FI Reported incident statistics

The NCSC-FI documents statistics for all incidents reported to the agency.

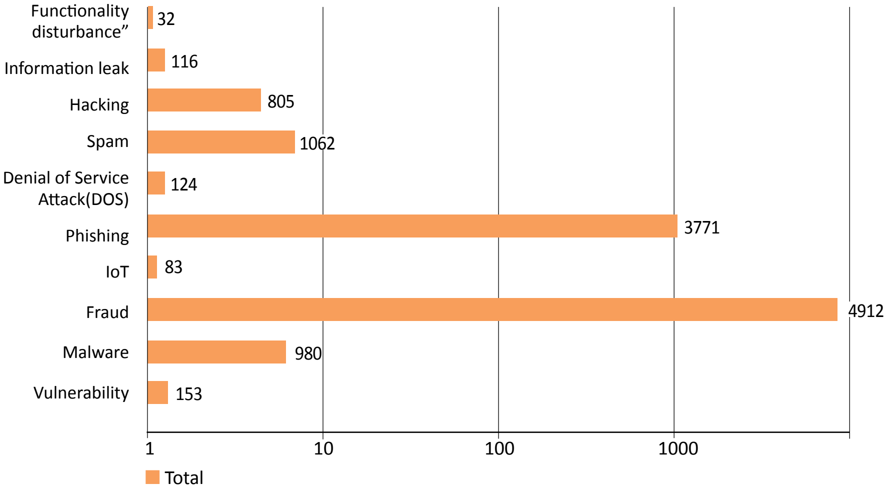
In the diagrams below we present the tota and logistic sector incident statistics by incident type for 2020.

Hacking, Phishing and Fraud incidents are the most common incidents in the logistics sector and a similar trend can be seen across the total reported incidents. In general, reports from the logistics sector are few compared to the other sectors. This does not necessarily mean that there are no security breaches in the sector, but rather that the NCSC-FI does not receive notifications from the organisations.

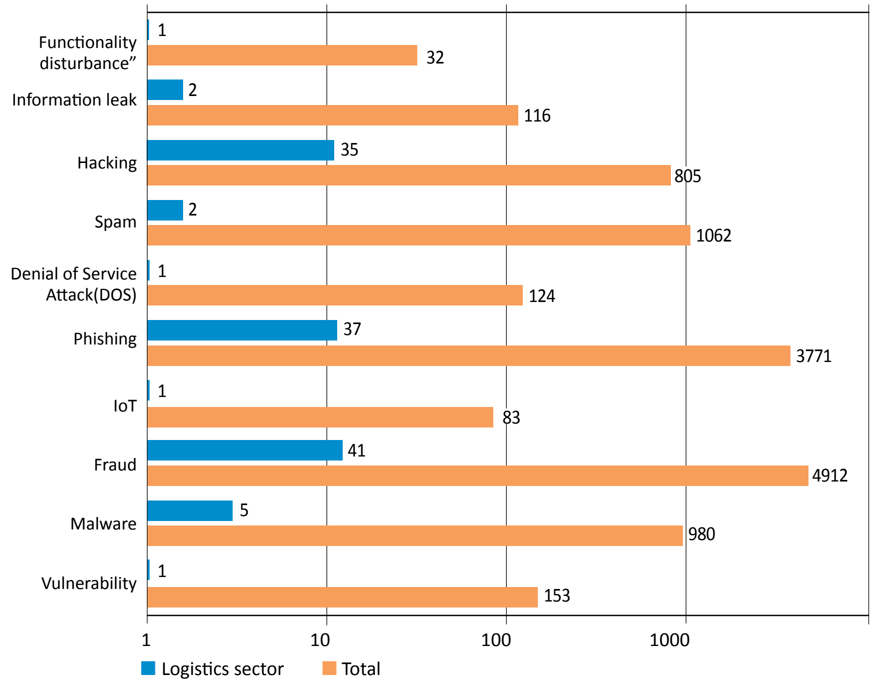
Reported incidents for logistics sector by incident type 2020



Reported total incidents by incident type 2020

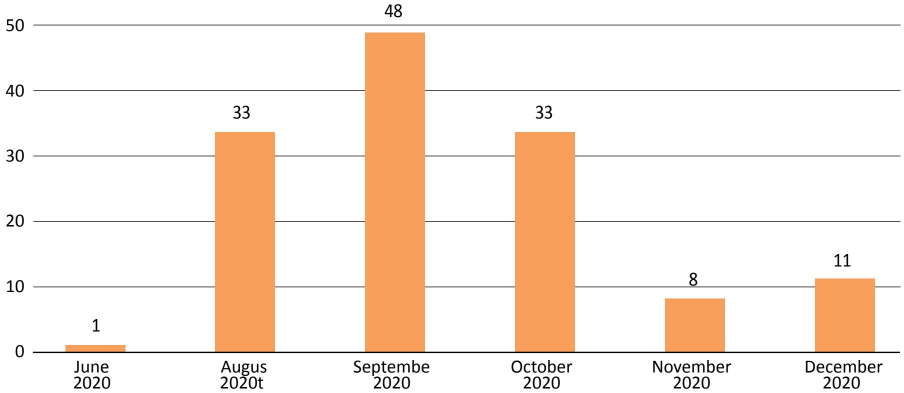


Reported incidentsby incident type 2020



The transport and logistics sector showed similar trends as other industries. Technical support scam calls have been a major scam during 2020. Finnish organizations and individuals have received a large number of calls during the early part of the year and during the summer, in which the caller appears as technical support. The caller claims that the victim's computer has a security issue and asks to open the machine to fix it. Scam calls are almost invariably made from foreign subscriptions. If a technical support scam targets an organization's employee or organization's tools, it will also compromise the organization's security and privacy. Another case that appeared especially in the latter part of the year was the Emotet malware. The NCSC-FI issued a serious warning about the spread of the Emotet malware in August 2020. During the autumn and early winter, the Emotet malware was distributed via e-mail via attachments on behalf of Finnish organizations.

Emotet malware reports per month 2020



The ISAC (Information Sharing and Analysis Center) is a cyber security co-operation body established for different industries. The transport and logistics sector has its own ISAC information exchange group. The Transport Operators Information Exchange Group (L-ISAC) shares information on cyber security threats, security breaches and phenomena in transport and logistics, and analyzes their impacts and safeguards across mode boundaries.

7.6. NCSC-FI references

Organisations in the maritime sector can freely use the services provided by the NCSC-FI to get relevant information regarding vulnerabilities, ongoing cybersecurity incidents and campaigns, weekly reports, etc. Links to the various services can be found below.

Information regarding the sector specific situational awareness information sharing and analysis centres (ISAC) can be found here:

- Situational awareness and network management

  FI: *https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen*

  SV: *https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap*

  EN: *https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management*

  ISAC group membership can be inquired by sending an email to *kyberturvallisuuskeskus@traficom.fi or ncsc-fi@traficom.fi*

- Cybersecurity and responsibilities of boards

  FI: *https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas*

  SV: *https://www.kyberturvallisuuskeskus.fi/sv/publikationer/cybersakerhet-och-styrelsens-ansvar*

  EN: *https://www.kyberturvallisuuskeskus.fi/en/publications/cyber-security-and-responsibilities-boards*

- Instructions and guides

  FI: *https://www.kyberturvallisuuskeskus.fi/fi/ohjeet*

  SV: *https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider*

  EN: *https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides*

- Cyberweather

  FI: *https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa*

  SV: *https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/cybervader*

  EN: *https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/cyber-weather*

- Situational awareness and network management

  FI: *https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen*

  SV: *https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap*

  EN: *https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management*

- Cybermeter / Kybermittari

  FI: *https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari*

  SV: *https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren*

  EN: *https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter*

- Tonttu-toteutettavuustutkimus -projektit
  https://www.kyberturvallisuuskeskus.fi/fi/tonttu

- ENISA:n Maritime-webpage
  https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/maritime

- ENISA cybersecurity guidance for ports
  https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-maritime-sector-enisa-releases-new-guidelines-for-navigating-cyber-risk

- ENISA Port Cybersecurity – Good practices for cybersecurity in maritime sector
  https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

- Safety4Sea – Cyber Security
  https://safety4sea.com/category/smart-parent/cyber-security

- The Maritime Executive
  https://www.maritime-executive.com/

  https://www.maritime-executive.com/features/securing-vessels-at-sea-frontline-insights-on-maritime-cybersecurity

- Maritime security centre of excellence
  https://www.marseccoe.org/en

- Maritime cybersecurity guidance by a commercial vendor Missionsecure:
  https://www.missionsecure.com/port-imo-cyber-risk-management-overview

8. APPENDIX B: CYBERMETER MATURITY LEVELS

A description of the management practices of each MIL can be found in the Traficom Cybermeter[37] and in the original Cybersecurity Capability Model (C2M2)[38] model listed below:

Maturity Indicator Level 0 (MIL0):

The model contains no practices for MIL0. Performance at MIL0 simply means that MIL1 in a given domain has not been achieved.

Maturity Indicator Level 1 (MIL1):

In each domain, MIL1 contains a set of initial practices. To achieve MIL1, these initial activities may be performed in an ad hoc manner, but they must be performed. If an organization were to start with no capability in managing cybersecurity, it should focus initially on implementing the MIL1 practices. MIL1 is characterized by a single management practice:

1. **Initial practices are performed but may be ad hoc**. In the context of this model, ad hoc (i.e., an ad hoc practice) refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of organizational guidance in the form of a prescribed plan (verbal or written), policy, or training. The quality of the outcome may vary significantly depending on who performs the practice, when it is performed, and the context of the problem being addressed, the methods, tools, and techniques used, and the priority given a particular instance of the practice. With experienced and talented personnel, high-quality outcomes may be achieved even if practices are ad hoc. However, at this MIL, lessons learned are typically not captured at the organizational level, so approaches and outcomes are difficult to repeat or improve across the organization.

Maturity Indicator Level 2 (MIL2):

Four management practices are present at MIL2, which represent an initial level of institutionalization of the activities within a domain:

1. **Practices are documented**. The practices in the domain are being performed according to a documented plan. The focus here should be on planning to ensure that the practices are intentionally designed (or selected) to serve the organization.

2. **Stakeholders of the practice are identified and involved**. Stakeholders of practices are identified and involved in the performance of the practices. This could include stakeholders from within the function, from across the organization, or from outside the organization, depending on how the organization implemented the practice.

[37] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_Cybermeter_User_Guide_V1.pdf
[38] https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

3. **Adequate resources are provided to support the process (people, funding, and tools)**. Adequate resources are provided in the form of people, funding, and tools to ensure that the practices can be performed as intended. The performance of this practice can be evaluated by determining whether any desired practices have not been implemented due to a shortage of resources. If all desired practices have been implemented as intended by the organization, then adequate resources have been provided.

4. **Standards and/or guidelines have been identified to guide the implementation of the practices**. The organization identified some standards and/or guidelines to inform the implementation of practices in the domain. These may simply be the reference sources the organization consulted when developing the plan for performing the practices. Overall, the practices at MIL2 are more complete than at MIL1 and are no longer performed irregularly or are not ad hoc in their implementation. As a result, the organization's performance of the practices is more stable. At MIL2, the organization can be more confident that the performance of the domain practices will be sustained over time.

Maturity Indicator Level 3 (MIL3):

At MIL3, the activities in a domain have been further institutionalized and are now being managed. Five management practices support this progression:

1. **Activities are guided by policies (or other organizational directives) and governance**. Managed activities in a domain receive guidance from the organization in the form of organizational direction, as in policies and governance. Policies are an extension of the planning activities that are in place at MIL2.

2. **Policies include compliance requirements for specified standards and/or guidelines**

3. **Activities are periodically reviewed to ensure they conform to policy**

4. **Responsibility and authority for performing the practices are assigned to personnel**

5. **Personnel performing the practices have adequate skills and knowledge**. The personnel assigned to perform the activities have adequate domain-specific skills and knowledge to perform their assignments.

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI