XAMK RESEARCH

MARITIME CYBERSECURITY

Before the risks turn into attacks

Vesa Tuomala

XAMK
South-Eastern Finland
University of Applied Sciences

Vesa Tuomala

MARITIME CYBERSECURITY

Before the risks turn into attacks

South-Eastern Finland
University of Applied Sciences

XAMK RESEARCH 18

SOUTH-EASTERN FINLAND UNIVERSITY OF APPLIED SCIENCES

KOTKA 2021

Cover picture: Vesa Tuomala
Layout and printing: Grano Oy
ISBN: 978-952-344-360-0 (PDF)
ISSN: 2489-4575 (ebook)
julkaisut@xamk.fi

Vesa Tuomala, Master Mariner (B.Sc.), Henley MBA, Project Manager

ABSTRACT

Cyber-attacks have increased during the CoVID-19 pandemic. There is an urgent need to understand the threats posed by cyber-attacks and identify how to minimise the potential risks. This study provides best practices to understand cybersecurity for the maritime industry. These best practices are a general awareness of cyber-attacks, the importance of defining roles and responsibilities, on board crew and ashore personnel readiness and preparedness drills for incidents in the shipping companies.

The hypothesis of this research is that the rate of maritime-related cyber-attack risk will continue to increase and as such, there is a need to raise awareness for the prevention and mitigation of incidents for the maritime stakeholders. Accordingly, the research question is: *What to do before risks turn into attacks in maritime cybersecurity?*

The research methodology was the study of new and relevant information from papers and articles written by cybersecurity experts. Accordingly, the research method was a literature review. This work is part of a larger desk study that aims to broaden the knowledge of cybersecurity and IoT issues of the maritime and logistics sector.

The research concentrates on the regulation governing cybersecurity, as well as privacy attacks conducted in 2020, information about the vessels, operational and control technology, and their cybersecurity. The research also focuses on how to prevent and mitigate cyber-attacks.

The discussion part outlines the research part and the findings of the best practices. The research concludes with the recommendation for further research on the next level of cybersecurity in future vessels and an investigation of the impact of INDUSTRY 4.0 on the logistics and maritime sector.

KEY WORDS: Maritime Cybersecurity, Risk Management, Maritime, Logistics, Ports

CONTENTS

1 INTRODUCTION

This desk study examines the benefits and threats of digitalization for the GET READY project in the maritime and logistics sector. The GET READY project is a cross-border cooperation between Russian and Finnish academic, scientific, and business partners. One of the project objectives is to search for best practices to avoid security incidents for vessels, shipping companies, port owners and operators.

The main objective of the GET READY project is to generate interest in increasing the awareness and readiness of environmentally sustainable development for the stakeholders on the vulnerable coastline. One of the objectives is to identify best practices for the development of the digitalization of port owners and operators, as well as shipping companies. This framework aims to create innovations for sustainable ports, protecting the environment, and mitigating climate change. The project implements capacity building in professional competencies via education and training, training content of digitalization of ports and smart ports, and managing environmental issues.

This desk study forms the third part of a research series concerning maritime digitalisation and cybersecurity. The first part "Logistics and maritime need to focus on cybersecurity in the Internet of Things (IoT) Technology" was published in Xamk Beyond in December 2020. The second part, "IoT productivity versus cybersecurity - is the risk worth it?" was published in May 2021.

The hypothesis of this research is that the rate of maritime-related cyber-attack risk will continue to increase and as such there is a need to raise awareness for the prevention and mitigation of incidents for the maritime stakeholders. Accordingly, the research question is: *What to do before risks turn into attacks in maritime cybersecurity?*

This desk study focuses on the cybersecurity challenges and defines the pertinent terminology of maritime cybersecurity. First, the study unpacks the research question and identifies the relevant issues and background information. Second, the current research and literature on cybersecurity are examined, along with international regulation and threats. These results will be examined to look for ways of preventing and minimizing the breaches, and decreasing the recovery time.

The third part of the study focuses on the discussion and identifies best practices to understand cybersecurity in the maritime industry. The study provides a general awareness of cyber-attacks and identifies the importance of defining roles and responsivities and awareness of crew on board and personnel ashore, also to organize drills for the preparedness for incidents in the shipping companies.

1.1 Hypothesis

Cyber-attacks have increased overall during CoVID-19 pandemic. On average a large cyber-attack resulting in stolen data or systems downtime is carried out against an organization every single week. This means, that identities and accesses need to managed and secure. No organization should operate on the assumption that it would not be the next one. In Finland, one of the latest and well-known cyber-attack on the health sector in Finland happened in 2018 and 2019, but the information was not released to the public until October 2020. The cyber-attack was a client database breach of confidential information from the Psychotherapy center Vastaamo. At the end of 2020, the Parliament of Finland also suffered an alarming series of targeted cyber-attacks, resulting in multiple compromised email accounts. (Ashton 2020; Passeri 2021.)

Safety at Sea and BIMCO noticed in their Maritime Cybersecurity Survey a 9 % increase of cyber-attacks influencing 31 % of organizations from February 2019 to February 2020. By the report of Naval Dome, the maritime industry's operational technology (OT) attacks increased 900% in three years, respectively 50 in 2017, to 120 in 2018 and 310 in 2019. (Tuomala 2020.)

The maritime cruise sector stores a considerable amount of customer information and financial data, which makes the industry particularly appealing to cyber-criminals. After a collision between an oil tanker and a US warship in 2017, the US government warns that cyber-criminals can sink cruise ships. (ShipTechnology 2020.)

The paper's hypothesis is that the rate of maritime-related cyber-attacks will continue to increase and as such there is a need to raise awareness for the prevention and mitigation of incidents for the maritime stakeholders. To address the hypothesis, I research international regulation and previous maritime cybersecurity incidents to see how interrelated these subjects are together. After that, I examine the information and operational technology of vessels' systems. My argument is that there is a gap between the cybersecurity know-how of the ship's crew and ashore personnel, and as such there is a strong need to understand cyber-attacks and prevent incidents in the future.

The study was carried out as a part of the Master of Engineer studies' Cybersecurity Audit and Cyber-hygiene of Maritime Cybersecurity. However, the reason to research cybersecurity is two-fold. On the one hand, I would like to help shipping organizations prevent incidents and mitigate the risks of data breaches. On the other hand, I am personally interested in gaining the latest knowledge and best practices on the subject, so that I can better teach future generations of students.

1.2 Research Methods

The research method is qualitative content analysis of open access research conducted by universities, researchers, companies, and professional organisations. In order to grasp a more holistic picture and to understand the cybersecurity threats to those devices used in the maritime sector, the study also utilises material from information and cybersecurity consultancy companies.

The research is qualitative and executed with the FINER method (Fandino 2019). The FINER criteria mean that research needs to be feasible, interesting, novel, and refuting, confirming, or developing previous research. In this context, feasibility means that there need to be enough subjects, technical expertise, and be manageable in scope. The research also needs to be carried out following ethical principles and be relevant. In this study, relevance focuses on scientific knowledge and researching the future. The FINER method is a very effective and suitable tool to research cybersecurity.

This paper proceeds as follows; I unpack the terminology used in this study and provide background information of the key terms. After reviewing the literature and data collection of the qualitative research, I examine the data in the research section. In the discussion section, I review the findings and analyse the gathered research information. The final part of the study concludes the issues raised and includes recommendations for further research.

2 DEFINING TERMINOLOGY

2.1 Definition of Cybersecurity

The British Cambridge Dictionary defines cybersecurity as “the things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet”, meaning cybersecurity ensures the protection of devices, networks, and data from unauthorized access.

The definition of information technology (IT) cybersecurity is based on the acronym “CIA” in the document of the European Union Agency for Cybersecurity, (hereinafter ENISA), which comes from the words ‘Confidentiality’, ‘Integrity’ and ‘Availability’. Information security means that the data should be under the preservation of confidentiality, integrity, and availability. Confidentiality means that the information is not available or disclosed to unauthorized individuals, entities, or processes. Integrity is related to accuracy and completeness. Availability means the property of being accessible and usable upon demand by an authorized entity.

After considering CIA, another core concept to explore is that of CAIC which relates to operational technology specifically. For operational technology (OT), the term CAIC stands for control, availability, integrity, and confidentiality. Control describes the ability to control a process, and to change the state safely and securely. The highest priority of controlling the processes impact safety, people, and assets in the attack of any system. (ENISA 2015; Mission Secure 2020.)

With this in mind, we can say that Information security means that the information is available when needed, is intact (original) and confidential, so that no one else can access it without permission. When these factors are all in hand, security risks are seen to be under control. Thus, information security is a key factor in cybersecurity, as it proactively enables the management of cyber threats and operations effects in the physical world. A security threat and the resulting event causes a cyber-disruption situation. A cyber threat or an event affects the cyber environment and can endanger the security of society. The cyber threat may be directed against vital societal activities, infrastructure, or domestic or foreign citizens. A cyber-attack is a realized cyber threat that endangers the operations of an organization or system. The management of cyber incidents can be divided into preparedness, situational awareness, prevention, and recovery. Cybersecurity means that the threats and risks to organizations’ necessary functions are under control. (Turvallisuuskomitea 2017.)

The main function of the cybersecurity process is to prevent damage to electronic information and communications systems, and preventing unauthorized use, exploitation and restoration of the information, computers, electronic communication systems and services, and wired communication. This enables the availability, integrity, authentication, confidentiality, and nonrepudiation of processes. As such, the cybersecurity process detects and responds to attacks and threats. (CSRC 2021.)

2.2 Definition of Risk Management

Risk management is a complete process of identifying, controlling, and eliminating or minimizing uncertain events to assets, operations and resources including mission, functions, image, or reputation and to individuals. The process is a security review that includes a risk assessment, cost-benefit analysis, and the selection, implementation, and testing of security and controls. Risk management also entails a mitigation strategy that responds to and continuously monitors the identified risks. The process includes effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations. (CSRC 2021.)

The Ministry of State in Finland describes risk management as a function that manages and controls organizational risks. According to the guidelines, risk means the effect of uncertainty on goals and a deviation from expectations. The impact of the risk can be positive or negative compared to what is expected. Simply put, risk refers to the impact of uncertainty on objectives. Risk can have a positive or negative effect, or both. It can concern people, animals, property, information systems, and the environment or community values. As such, risks are a deviation from expectations that creates opportunities or threats. Risk assessments are performed to be able to prepare for different threat models. Threat models are refined and updated through continuous and regular risk assessments. Risk management is systematic and goal-oriented operations, organizational management, and development. (Rousku 2017; Turvallisuuskomitea 2017.)

According to the Ministry of Finance of Finland, risk management assesses the risks that an organization takes in setting strategic goals and how they are managed. Projects will succeed by ensuring good risk management. Risk assessments must be carried out in day-to-day work and when there are significant changes to a system. According to the guide, many risks cannot be eliminated, so the consequences must be prepared for in advance. Risk management necessitates cooperation with the different stakeholders involved and includes risk analysis and measures taken to plan, implement, monitor, and correct the situation. In addition to taking a risk, there are other ways to avoid or shift it. If necessary, the risk can be reduced by sharing it or by preventing damage. Adequate resources for operations must be determined in risk management. (Rousku 2017; Turvallisuuskomitea 2019.)

2.3 Definition of Threat and Attack

A threat are harmful actions or attempted actions to an organization and its operations and resources including mission, functions, image, or reputation and to individuals. A threat can be the unauthorized access, destruction, disclosure, modification of information, and/or denial of service to the information system of the organization. This is slightly different to an attack, as the purpose of an attack is disrupting, disabling, destroying, or maliciously controlling an organization's infrastructure or information systems in cyberspace. The attack can destroy the integrity of the data or steal controlled information. (CSRC 2021.)

I have opened and explained the core terminology of cybersecurity, risk management, threat, and attack. It is now time to move onto the research part of the paper.

3 RESEARCH

The Government Resolution on Finland's maritime policy guidelines From the Baltic Sea to the oceans outlines automation, digitalisation and data, expertise, research and education related to cybersecurity in Finnish maritime policy. The main objectives are to reduce the number of maritime accidents, ensure the quality and timeliness of navigation data, develop maritime shipping for autonomous vessels, promote digitalisation in logistics chains, develop advanced interfaces for reporting methods, improve autonomous vessels and promote autonomous maritime transport in the European Union. (Prime Minister's Office 2019.)

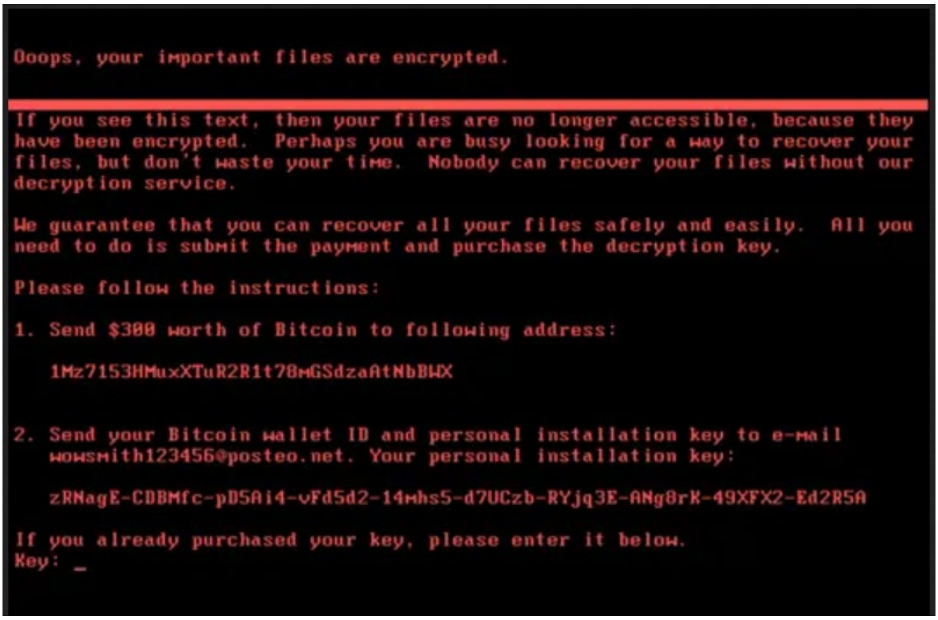
The topics I cover here include cybersecurity regulation in the maritime sector and attacks during 2020 as well as future cybersecurity threats. I shall focus on the vessel's operational technology and consider how to build cybersecurity and design secure fleets.

3.1 Cybersecurity Regulation in the Maritime Sector

The International Maritime Organisation (hereafter IMO) regulates international shipping and global standards for safety and security. In June 2017, the IMO informed the shipping stakeholders of the cyber risk threats and vulnerabilities in the resolution Annex 10 in MSC.428 (98). The annex is for member states administrations, classification societies, ship-owners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders. It affirms the need for cyber risk management and encourages that concrete steps are taken in this area, acknowledges the necessary precautions, and requests that all stakeholders are made aware of this resolution. (Tuomala 2020.)

The real revelation about the potential harm of the cyber threats in the maritime sector was the ransomware notPetya and an attack against the whole A.P. Møller-Maersk company on 27th June 2017. The cyber-attack did not explicitly target the Maersk organization, instead NotPetya targeted mainly Ukraine and was traced to an accounting software package that spread to Maersk's infrastructure. NotPetya was an aggressive and damaging piece of ransomware. It used advanced infiltration and lateral movement to infect systems. Ransomware is malware that is specifically designed to stealthily infiltrate PCs, mobile devices, and even Industrial Control Systems. NotPetya caused destruction; it influenced every single domain-joined Maersk's Windows laptop, desktop, virtual machine, and physical server around the world. Malware takes control of a device and locks access. After that, the ransomware demands payment in an untraceable digital currency, called cryptocurrency. The impacts of a cyber-attack are more significant than they appear in the headlines. This incident pushed The International Maritime Organisation (IMO) to realize that the shipping sector is vulnerable to cyber-attacks. (Ashton 2020; Nettitude 2019.)

The screenshot below is from a device at Maersk that was infected with the ransomware notPetya. It explains to the user that all the important files on the computer are encrypted and gives the user instructions on how to pay the ransom to a Bitcoin account. The message instructs the user to pay 300 U.S. dollars to a specified account and send the users' Bitcoin identification information to the attacker's email address.



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.
Key: _
```

Picture 1: Encrypted Maersk screen with notPetya around the world by Gavin Ashton, 27th June 2017

The IMO stated that maritime cybersecurity belongs to existing Safety Management Systems (SMS) under the International Safety Management (IMS) Code. The IMO issued guidelines on maritime cyber risk management in the MSC-FAL.1/Circ.3. This document enforces those cyber risks are appropriately addressed in existing shipping company's Safety Management System (SMS) of ships. This need to be in company's Document of Compliance after 1 January 2021. (Tuomala 2020.)

The IMO also regulates port safety and security with the International Ship and Port Facility Security (ISPS) code. The ISPS includes procedures for physical security on ports, and protecting underway, berthed, and docked vessels. The ISPS also states how to develop a cybersecurity assessment (CSA) and a cybersecurity plan (CSP). The ISPS Code ratified by the European Commission (EC) Regulation 725/2004 into the EU Law. (European Union 2004; Tuomala 2020.)

3.2 Cybersecurity and Privacy Attacks of 2020

Cyber-attack targets have been conducted against for example, multiple industries, individuals, public administration, defence, social security, health, education, and the financial and insurance sector. There have been several major recognized incidents against the maritime sector. (Passeri 2021.)

In March 2020, an attack on the Norwegian Cruise Line resulted in a data breach of 29,969 records. The breached database that connected their travel agent partner portal was discovered on the dark web. Two Carnival Cruise Line cruise ships received email phishing attacks; the incident focused on customer and employee data. In April 2020, the world's second-largest container line Mediterranean Shipping Co (MSC) was hit by a malware cyber-attack that caused a data centre outage resulting in the primary customer websites and the Geneva Headquarters being shut down for five days. Additionally, the Carnival Cruise Line, Holland America Line and Seabourn from Carnival Corporation had ransomware cyber-attacks, that gained access to guest and employee personal data in the middle of August. There was a malware attack on Overseas Express Shipping Company in the middle of September. The ransomware attack on the French maritime transport and logistics company CMA CGM S.A hit at the end of September and there was an unknown attack on the IMO at the beginning of October 2020. In the middle of December, there were major ransomware attacks on Hurtigruten, Norwegian Cruise Company that closed several key systems down and affected its global IT infrastructure. German AIDA Cruises, including ships AIDAmar and AIDAperla, had a mysterious IT restriction at the end of the year and had to cancel New Year's Eve cruises. The incident also affected AIDA's cruise line operations resulting in the failure of the company's computer and internet systems, and land-based and shipboard telephones. (Passeri 2021; Reuters 2020; ShipTechnology 2020; Walker 2020.)

3.3 Future Cybersecurity Threats

Security must be an enabler – not an inhibitor, says Mika Laaksonen, Head of Technology Advisory Services in multinational professional services network company KPMG. He predicts the next trends for the 2020s and identifies that there is a need for experts that have technical and business skills to solve cybersecurity issues. Additionally, there need to be user-friendly and strong solutions for authentication and password policies, and risks for different industries need to be identified. Systematic risks may realise outside of their own organization, meaning that cybersecurity strategies need to cover the entire value chain, and data recovery and protection is important. In cloud-based solutions, Laaksonen believes that identity confirmation will be the key focus in the upcoming decade. (Laaksonen 2020.)

Cybercriminals have evolved to use ransomware with phishing emails or embedded in malicious webpages. Infected organisations, which use backups, may recover more quickly. Nowadays ransomware does not launch an encryption attack right away, but it continues to communicate under the command and control of the attacker. The attacker may laterally filter data before encryption, or ransomware can be used as a backdoor for carrying other tools for searching valuable or sensible information in the organisation's systems. Ransomware can also be a strategy to hide evidence of a more serious incident. A Distributed Denial-of-Service (DDoS) attack is used in the same way to hide tracks of an attack. Malware attacks can be used to delete event logs and avoid detection. (Prevailion no date; Swinhoe, D. 2019.)

3.4 Cyber Secure Vessels and Organisations

The IMO has set new regulations concerning maritime cyber risks management as guidelines for managers, operators, and owners in the document MSC-FAL.1/Circ.3. The regulations highlight the importance of automation, digitalization, and technology to increase the performance of the maritime industry. Modern ships will have more automation through connected and integrated systems with diverse components and interfaces, and a complex supply chain. These ships need expertise and knowledge with assurance and verification. In practice, managing modern ships mean less personnel and more automation. Older ships will have more cybersecurity vulnerabilities and weaknesses with critical functions of Industrial Control Systems (ICS), automated navigation, onboard inventory, and management software.

From a security perspective, newer ships have better design, patching and configuration than older ships. Vessels need to be cyber secure entities. Cybersecurity needs to be at a high level to ensure the safety and security of the ship, crew, passengers, and cargo at the same time with the new technological innovations. The number of cyber threats is increasing in the shipping and offshore sector along with potential attacks on the vessels operational and control systems. Both cyber safety and cybersecurity means protection for personnel, and the ship and its cargo against unauthorised access to the information and data, and manipulation and distribution of the ships' Information Technology (IT) and Operational Technology (OT) systems.

The unwanted cybersecurity incident risks the loss of availability and integrity, failures for software maintenance and the loss of sensor data. These could lead to losing sensitive and personal data, or in the worst case to loss of life or the entire ship. IT consists of electronics, computer systems (personal computers, laptops, tablet devices, servers, routers, and switches) and wireless systems, and information, services, social and business functions. IT systems have combined procedures, technology and training against cyber criminality and data breach results in financial and reputational losses and do not affect the safe operation of vessels. OT is used for direct sensing, monitoring and control of physical devices as motors, pumps and valves in machinery, communications, sensors, and navigation systems. Ships have navigation systems, communications, and integrated bridge computers. Ships also have control systems to manage engines, propulsion, steering, generators, and ballast, bilge, freshwater, fuel and oil pumps, watertight doors, fire alarm systems, cargo hold fans and environment space systems are crucial for operating the ships. Whereas an attack on a ship's IT systems cannot endanger life or its safe operation, an attack on a vessel's OT system risks the crew and passengers' safety. Cyber criminality may result in a massive financial risk for the shipping company. (Bimco et al.; Boyes 2013; Department of Transport 2017; DNV GL 2016; DNV GL 2020; Nettitude 2019.)

The critical functions on older ships have more cybersecurity vulnerabilities and weaknesses with their Industrial Control Systems (ICS). The National Institute of Standards and Technology (NIST) has issued guidance for the unique performance, reliability, and safety requirements to secure ICS, Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). The ICS are designed and implemented with connectivity and remote access capabilities on industry-standard computers, operating systems (OS) and network protocols with Internet Protocol (IP) devices, will increase the possibility of cybersecurity vulnerabilities and incidents. An ICS may confront the following possible incidents (NIST 2015.):

- Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation.

- ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects.

- Inaccurate information sent to system operators, either to disguise unauthorized changes or to cause the operators to initiate inappropriate actions, which could have various negative effects.

- Interference with the operation of equipment protection systems, which could endanger costly and/or difficult-to-replace equipment.

- Interference with the operation of safety systems, which could endanger human life.

- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life.

The guidelines on cybersecurity for onboard ships includes a comprehensive summary list of potentially vulnerable target systems, equipment and technologies, and data onboard ships. The risk can be environmental, financial, reputational, and to life or property. Vulnerable systems, equipment and technologies can be as follows (Bimco et al. 2020; Mission Secure 2020; Nettitude 2019.):

Access control and safety systems

- Bridge Navigational Watch Alarm System (BNWAS)
- Electronic "personnel-on-board" systems
- Emergency shutdown
- Fire and flood control
- Physical access control as locks and doors
- Tracking
- Shipboard Security Alarm Systems (SSAS)
- Surveillance systems such as CCTV network

Administrative, supply chain and crew welfare systems

- Administrative and email systems, fax
- Automated manifest
- Crew Wi-Fi or LAN internet access
- Consumable stores inventory
- Customs and immigration handling
- Bring Your Own Devices (BYOD) for personnel connections
- Maintenance and spares management
- Remote and onshore vendor updates
- Timekeeping and scheduling

Bridge control systems

- Automated weather monitoring
- Automatic Identification System (AIS)
- Automatic Radar Plotting Aid (ARPA) and radar equipment
- Electronic Chart Display Information System (ECDIS)
- Dynamic Positioning (DP) systems
- Global Maritime Distress and Safety System (GMDSS)
- Global Navigation Satellite and Positioning Systems (GPS, Glonass)
- Integrated navigation system
- Other monitoring and data collection systems
- Systems that interface with electronic navigation systems and propulsion/manoeuvring systems
- Voyage Data Recorders (VDRs)

Cargo management systems, loading and stability

- Ballast water systems
- Bay and stowage planning
- Cargo Control Room (CCR) and its equipment
- Cargo management systems
- Hull stress monitoring
- Level indication system
- Stability control and decision support systems
- Valve remote control system
- Water ingress alarm system

Communication systems

- Integrated communication systems, intercom
- Public address and general alarm systems
- Satellite communication equipment
- Ship-to-shore and ship-to-ship communications, handheld radios
- Voice Over Internet Protocols (VOIP) equipment
- Wireless networks (WLANs)

Passenger-facing networks

- Guest entertainment systems
- Passenger Wi-Fi or Local Area Network (LAN) internet access, for example where onboard personnel can connect their own devices

Passenger servicing and management systems

- Electronic health records
- Financial related systems
- Infrastructure support systems like domain naming system (DNS) and user authentication/authorisation systems
- Property Management System (PMS)
- Ship passenger/seafarer boarding access systems

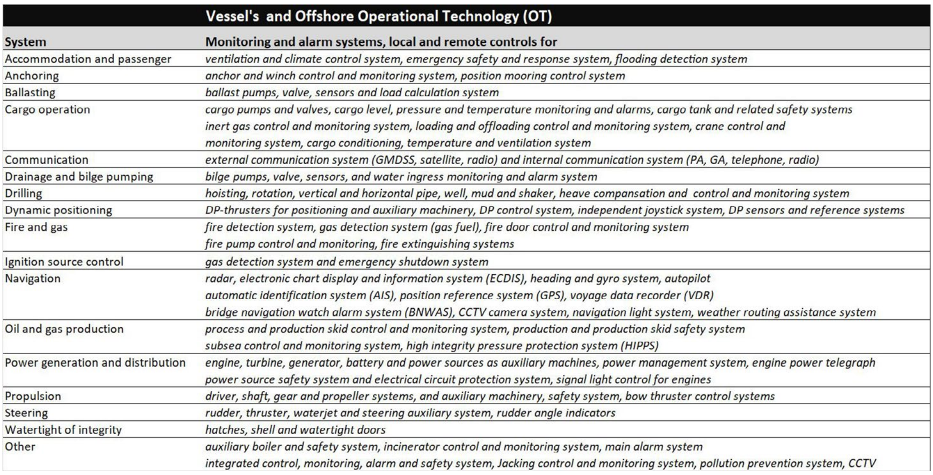
Propulsion and machinery management and power control systems

- Alarm system
- Emergency response system
- Engine governor and control
- Generators
- Integrated control system
- Onboard machinery monitoring and controls
- Power management
- Steering

Operations, network and physical security, ICS systems

- Antivirus software, software updates and vendor patches
- Bridge and machinery space restriction
- Digital and analogue sensors
- Electronics and electrical management
- External data storage devices (USB, DVD/CD, portable HDD)
- Firewalls
- Human-Machine Interfaces (HMIs)
- Intrusion prevention systems
- Programmable Logic Controllers (PLCs)
- Routers, switches and other segmentation devices
- SCADA controllers
- Security gateways
- Security event logging systems
- Server rooms, access control barriers
- Virtual LANs (VLAN)
- Virtual Private Networks (VPN)

Ships and offshore supply vessels have many different systems for the Operational Technology (OT). The table below explains which kinds of monitoring and alarm systems for local and remote control are needed to operate technology on ships:



	Vessel's and Offshore Operational Technology (OT)
System	**Monitoring and alarm systems, local and remote controls for**
Accommodation and passenger	*ventilation and climate control system, emergency safety and response system, flooding detection system*
Anchoring	*anchor and winch control and monitoring system, position mooring control system*
Ballasting	*ballast pumps, valve, sensors and load calculation system*
Cargo operation	*cargo pumps and valves, cargo level, pressure and temperature monitoring and alarms, cargo tank and related safety systems* *inert gas control and monitoring system, loading and offloading control and monitoring system, crane control and monitoring system, cargo conditioning, temperature and ventilation system*
Communication	*external communication system (GMDSS, satellite, radio) and internal communication system (PA, GA, telephone, radio)*
Drainage and bilge pumping	*bilge pumps, valve, sensors, and water ingress monitoring and alarm system*
Drilling	*hoisting, rotation, vertical and horizontal pipe, well, mud and shaker, heave compansation and control and monitoring system*
Dynamic positioning	*DP-thrusters for positioning and auxiliary machinery, DP control system, independent joystick system, DP sensors and reference systems*
Fire and gas	*fire detection system, gas detection system (gas fuel), fire door control and monitoring system* *fire pump control and monitoring, fire extinguishing systems*
Ignition source control	*gas detection system and emergency shutdown system*
Navigation	*radar, electronic chart display and information system (ECDIS), heading and gyro system, autopilot* *automatic identification system (AIS), position reference system (GPS), voyage data recorder (VDR)* *bridge navigation watch alarm system (BNWAS), CCTV camera system, navigation light system, weather routing assistance system*
Oil and gas production	*process and production skid control and monitoring system, production and production skid safety system* *subsea control and monitoring system, high integrity pressure protection system (HIPPS)*
Power generation and distribution	*engine, turbine, generator, battery and power sources as auxiliary machines, power management system, engine power telegraph* *power source safety system and electrical circuit protection system, signal light control for engines*
Propulsion	*driver, shaft, gear and propeller systems, and auxiliary machinery, safety system, bow thruster control systems*
Steering	*rudder, thruster, waterjet and steering auxiliary system, rudder angle indicators*
Watertight of integrity	*hatches, shell and watertight doors*
Other	*auxiliary boiler and safety system, incinerator control and monitoring system, main alarm system* *integrated control, monitoring, alarm and safety system, Jacking control and monitoring system, pollution prevention system, CCTV*

Picture 2: Combined Vessel's Operational Technology Systems, modified from Bimco et al.; Boyes 2013; Department of Transport 2017; DNV GL 2016; DNV GL 2020

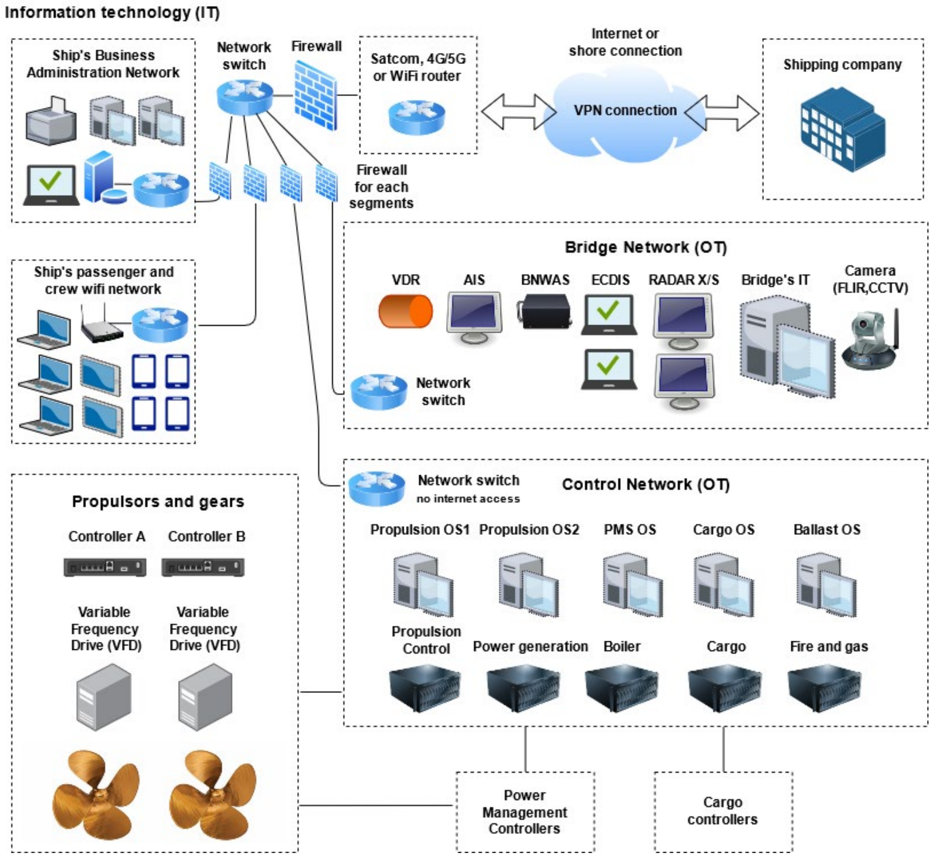
3.5 Prevent Breaches, Decrease Recovery Time

Cyber-attacks on Industrial Control Systems (ICS) environments and their automation components are no longer fiction but reality. Cybersecurity becomes more important as organizations digitize operations. Critical software and firmware updates minimize overall cybersecurity risks. The operational personnel need to backup all critical files, software, and data, as this is essential to decrease the time of recovery. (Kaspersky 2020; U.S. Coast Guard 2019.)

The entire organization needs to commit to safety protection policies that prevent cyber-attacks and threats. The company needs to have clear procedures for operating normally and in emergencies, that states the clear roles, tasks and responsibilities for onboard crew and staff ashore. Staff training programmes need to include competence assessments for cybersecurity problems. The organization should have a programme that is continuously improved and updated. (DNV GL no date; U.S. Coast Guard 2019.)

More than likely, cybersecurity was not a serious consideration when many older ships were constructed. However, over the years, many IT systems have probably been installed afterwards on older ships. Thus, it is necessary that communication should be prevented between a controlled and uncontrolled network with various encryption protocols, verification certificates, separation, and traffic management. IT and OT systems should include risk management for identifying threats, vulnerabilities and weaknesses, assessments of possible incidents and effective protection, and system maintenance for cybersecurity and cyber safety. IT and OT system networks, as well as public network segmentation, are necessary to prevent entries in the other's environment with cabling, firewalls, switches, and servers. Such as, physical security restrictions and controlled entry points to the networks. Administration and managing the network requires software on workstations and servers for email, file sharing and printing. Firewalls between each segmented networks, Virtual Local Area Networks (VLAN) and own range of Internet Protocol (IP) addresses are required for hosting separated segments. Each segment should have software firewalls, malware detection and network access control. IT and OT network diagrams need to be up to date for securing different elements. Real-time network traffic monitoring with Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) help to mitigate the risks of penetration. Centralized and monitored host and server logging need to be in use for alerting the misuse of networks. (DNV GL no date; U.S. Coast Guard 2019; Mission Secure 2020.)

The example below of network topology from a fictional onboard vessel shows segmented four VLAN's with firewalls, separating IT and OT networks with routers, and crews and passenger entertainment networks. The IT network is for administrative and business functions and the OT network is for safety-critical functions. (Bimco et al. 2020; DNVGL; NIST 2015.)



Picture 3: Simplified vessels' network topology, modified from Bimco et al., DNVGL and NIST 2015

The members of the organization's cybersecurity team should consist of IT staff, a control engineer, a control system operator, a network and system security expert, a member of the management staff, and a member of the physical security department at the bare minimum. Additionally, the cybersecurity team should contact the control system vendor and system integrator. Accordingly, the ICS implementation should include the following security objectives (NIST 2015):

- Detecting security events and incidents, failed ICS components, unavailable services, and exhausted resources.

- Maintaining functionality during adverse conditions, where each critical component has a redundant counterpart.

- Protecting individual ICS components from exploitation, deploying security patches as expeditious, disabling all unused ports and services, restricting user privileges, tracking and monitoring audit trails, and using antivirus software and file integrity checking software to prevent, deter, detect, and mitigate malware.

- Restoring the system after an incident. Incidents are inevitable and an incident response plan is essential. A major characteristic is how quickly the system can be recovered after an incident has occurred.

- Restricting logical access to the ICS network, and network activity with unidirectional gateways, a demilitarized zone (DMZ) network architecture with firewalls and a multiple-layer network topology.

- Restricting physical access to the ICS network and devices with the combination of physical access controls as locks, card readers, and/or guards.

- Restricting unauthorized modification of data.

From the lessons learned from the ransomware notPetya attack to Maersk organization, a layered approach is required to reduce threats. NIST describes their Five Functions of the best practices for a successful and holistic cybersecurity programme and maintaining the management systems systematics from a technological perspective. In this, an organization can manage cybersecurity risks and make calculated risk management decisions with this tool. (Ashton 2020; NIST 2018; Traficom 2020):

Identify • Protect • Detect • Respond • Recover

1. Identify the organization's systems and people, assets, capabilities, and data. Understand the possible risks in the IT and OT systems.

2. Protect all critical infrastructure services and limit a possible cybersecurity incident. Protect identity and access control.

3. Detect and discover the occurrence of a cybersecurity event. Educate personnel with user training and empower awareness for protecting confidentiality, integrity and availability of information.

4. Respond with appropriate activities regarding a detected cybersecurity incident and contain the impact of a potential cybersecurity incident. Use response planning process and mitigate the event, resolve the incident.

5. Recover appropriate activities to maintain resilience and to restore services. Recover to normal operation.

DNV GL recommends a quick checklist for maritime cybersecurity based on the IMO's International Safety Management Code (ISM Code) and the MSC/FAL.1/Circ.3. The list creates awareness and focuses on cybersecurity with reference to the appendix of the Safety Management System (SMS). The list is as follows (DNV GL no date):

- Adequate resources and ashore support of handling cybersecurity enabled to designated persons.

- All levels of the organization (ashore and onboard) have an implemented and maintained cybersecurity policy.

- Continuous improvement for safety management skills of personnel (ashore and onboard vessels), including preparing for emergencies and cybersecurity breaches:
  - Cyber drills,
  - Familiarization and instructions of cybersecurity duties,
  - General cybersecurity awareness training,
  - Procedures for identifying training needs, execution of training and distribution of relevant information,
  - Task and role-specific cybersecurity training.

- Cybersecurity to be included in all procedures, plans, instructions, and checklists for key onboard operations concerning the safety of the personnel, ship, and protection of the environment.

- Cybersecurity events which may lead to emergency situations onboard are identified and response procedures are established:
  - Cyber incident response procedure,
  - Program for cyber incident response drills,
  - Other measures supporting 24/7 effective response-

- Cybersecurity non-conformities, accidents and hazardous situations are reported to the company:
  - Defined responsibilities and tasks related to who is reporting a cyber-incident,
  - Procedure for cyber incident reporting,
  - Training for cyber-related incident reporting.

- Documentation and definition of responsibility, authority and interrelation to all personnel working with cybersecurity.

- Establish and maintain procedures to control all documents and data of the Safety Management System (SMS), including cybersecurity.

- Following compliance regulations.

- Identified risks and objectives to ships, personnel, and the environment with appropriate safeguards.
- The ship's master's responsibility needs to be defined and documented:
  - Implementing cybersecurity measures in the Safety Management System,
  - Issuing orders and instructions on cybersecurity in a clear and simple manner,

  - Motivating the crew in the observation of the measures,
  - Periodically reviewing the SMS and reporting its deficiencies to the shore-based management,
  - Verifying that cybersecurity requirements are observed.

- Master has the overriding authority and the responsibility to make decisions with respect to safety and pollution prevention, including on cybersecurity, and to request the organization's assistance when necessary.

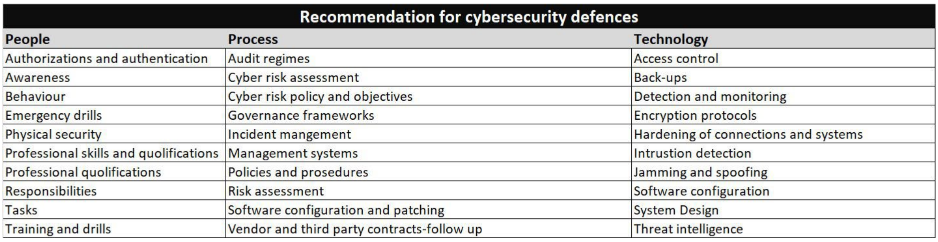
- Procedures and activities are implemented to identify and execute corrective action, including to prevent the recurrence of cyber incidents and non-conformities:
  - Follow up on reports and analysis of non-conformities, incidents and threat intelligence,
  - Internal cyber risk audits, assessments and tests,
  - Management review,
  - Master's review with cybersecurity on the agenda,
  - Reporting and analysis systems.

- Safe practise, operation. and working environment in all areas

- Considering applicable codes, guidelines, and standards recommended by the IMO, and other administrations, classification societies and maritime industry organizations.

- Ensuring the link between ashore and onboard personnel regarding cybersecurity

DNVGL summarises the recommendations for cybersecurity as follows:



Recommendation for cybersecurity defences		
People	**Process**	**Technology**
Authorizations and authentication	Audit regimes	Access control
Awareness	Cyber risk assessment	Back-ups
Behaviour	Cyber risk policy and objectives	Detection and monitoring
Emergency drills	Governance frameworks	Encryption protocols
Physical security	Incident mangement	Hardening of connections and systems
Professional skills and quolifications	Management systems	Intrustion detection
Professional quolifications	Policies and prosedures	Jamming and spoofing
Responsibilities	Risk assessment	Software configuration
Tasks	Software configuration and patching	System Design
Training and drills	Vendor and third party contracts-follow up	Threat intelligence

Picture 4: Recommendations for cybersecurity, modified from DNVGL

One way to building trust from the bottom-to-up level is to engage with people and listen to them, and to trust the professional employees' expertise of cybersecurity. The connection between human capital and cyber risk needs to be established and developed. An organisation has a duty of care to its customers, employees, contractors and partners. The principles found after the 2017 notPetya attack on Maersk were as follows (Ashton 2020):

- 70 per cent of cyber risk events start with a compromised identity.
- A decentralised approach will see individual systems report data in and minimising exposure of the entire environment to a particular account.
- Any systems not patched, consider using an automated quarantine process and make the application owners accountable.
- Priority action to the operating systems that are out of the support cycle as they represent a critical vulnerability for the core business.
- Do not delay security patches and updates.
- Maintain a list of priority business-critical applications.
- Multi-Factor Authentication (MFA) and password protection manage the major threats to identities.
- The connection between human capital and cyber risk needs to be established.
- Without data, it is impossible to demonstrate the scale of the issue and plan an approach.

Supply chains have increased challenges with manufacturers, IoT devices, sensors and automation technology. Ships gather considerable data from the functions, navigation, positioning, logistics, cargo, and safety of vessels. Communication systems. ashore operations and ports may create major disruptions with IT malfunction in the complex logistic supply chains. Threats may vary from nation-states jamming GPS signals, pirates investigating cargo onboard and undetected ports, drug cartels moving products, untargeted malware attacks to terrorist activity. A large task should be transforming systems into the new technology of Industry 4.0 to generate significant cost savings and increased efficiency. The balance of the ease of use of automation, Big Data analytics, cloud services, industrial IoT technology and next-generation management systems needs to be considered. The other perspective is the need of building and designing secure fleets, as well as an operational fleet management perspective. The shipping sector interacts with different entities for scheduling, loading of cargo, personnel assignment, cargo and loading docks, harbourmasters and port authorities to ensure vessels reach their destinations safely and promptly. Awareness of cyber threats and an effective cybersecurity strategy make it possible for organisations to adopt automation, cloud services, connectivity, IoT, and Industry 4.0 technology with increased security and protection. (Nettitude 2019.)

Database security and identity management would benefit from differentiation of the IT/OT system. Navigation systems are mission-critical applications and need to be available continuously. Protecting identity and access control these systems with Multi-Factor Authentication (MFA) is not always possible.

4 DISCUSSION

Cyber-attacks are a reality. Statistics confirm that cybercriminal activity has been increasing during Covid-19 by Interpol.

Seafarers need to understand the importance of cybersecurity and have a comprehensive understanding of the different vulnerabilities, risks and cybersecurity controls of the vessels, shipping companies, and their systems.

Automation and navigation systems onboard are mission-critical applications. Safe patching of these systems are not able to do during operations, due to the patch needs verification from vendor. It is also impossible to set these systems into quarantine during use of them.

An organization's ability to take risks to achieve strategic goals is examined through risk assessment, which is performed in day-to-day work and when there are significant changes. Risks cannot be eliminated entirely, so the consequences must be prepared for or mitigated in advance. Risk management includes risk analysis and measures to implement the plan, as well as monitoring and correcting situations as they arise. Risks can be avoided, transferred, reduced or prevented. Risk management determines the sufficient resources needed to take measures. The risk can be environmental, financial, reputational and to life or property.

A threat or cyber-attack on an organization can adversely affect its resources, missions, image and reputation, and the actions of an individual. Cyber threats occur through intrusions, destruction, disclosure and alteration of information or denial of access to an organization's information systems. The purpose of attacks is to disrupt, disable, destroy, or control an organization's infrastructure or information systems in cyberspace. Attacks can destroy data integrity or steal managed data.

The real revelation in the shipping industry was the aggressive and damaging notPetya ransomware which paralysed the shipping industry. In the year 2020, cyber-attacks targeted several industries, including public administration, defence, social security, health, education, finance and insurance, and individuals. According to statistics, several significant cyber-attacks targeted the shipping industry and it appears that maritime cyber-attacks will continue to increase in the future, as I have noticed in my earlier IoT cybersecurity research. There is a need to increase awareness and training of maritime stakeholders in the prevention and mitigation of attacks. There is also a need for cyber-security experts who understand the processes of the whole value chain, strategies for authentication, password policy, protection and data recovery. Cybercriminals may use ransomware, phishing emails, malicious webpages, and DDoS attacks to hide evidence and tracks and might also deleting event logs of more serious incidents.

Cybersecurity needs to be at a high level due to the increasing automation, digitalization, and technology to ensure ship, crew and passenger safety. Increasing cyber threats and potential attacks on the vessels' information, operational and control systems risk life, and the loss of sensitive and personal data, as well as potentially resulting in the loss of the whole ship. Operational and control systems include bridge, cargo, communication, engine's propulsion, machinery and power control systems, as well as passenger's management and service systems, administration and crew's welfare systems. Digital systems onboard and ashore are used for managing and controlling cargo and hazardous materials with shipment-tracking tools via the internet. Bridge and engine operational systems, even those that do not have an internet connection are vulnerable when updating and patching systems using external hard disks, DVDs and USB memory sticks. These systems may be particularly attractive to cybercriminals and attacks.

All service denial attacks and manipulations affect navigation, propulsion, steering, machinery and power control systems. Cyber-attacks may risk the safety and security onboard. In the future, these systems are remotely connected ashore for the autonomous shipping.

Due to the massive amount of personal data, ships' access control systems for physical security and surveillance camera systems and passenger management and service systems may be fascinating to cybercriminals. Additionally, the passengers have their intelligent devices as personal computers, tablets and mobile phones with them. As such, the crew will also need to have their own separate connection to the internet without access to the ships' information and operational network.

The lessons learned from the Maersk incident is that an attack can come from the outside of the shipping company's own network through the patching of any software system. Satellite and wireless systems are not safe due to the open networks, spoofing and jamming signals. As the saying goes, locks are only for honest people.

Best Practices

Industrial Control Systems (ICS) are a potential security risk for cyber-attacks. An organization needs to have a cybersecurity strategy, based on identified risk analysis, which defines the trusted state when the information, operating and control systems are secure, defended, contained, monitored, and managed. Based on the research conducted, I gathered a list of the best practices for preventing attacks:

- **Application security**

A list of priority critical applications needs to be maintained. The systems need to be up-date with the critical software patches, applied without delay. The use of file integrity software should prevent, deter, detect and mitigate malware. Third-party applications may result in a cybersecurity incident and unpatched systems need to put quarantine.

- **Database security and identity management**

Systems and assets need to documented and people have a responsibility for security. Data needs to have restrictions placed on unauthorized modification. Track and monitor audit trails. Protect identity and access control with Multi-Factor Authentication (MFA) and password protection for managing the threats to identities. Restrict user privileges and monitor activity.

- **Endpoint security**

Use appropriate anti-virus software. Ensure the crew, passenger, and entertainment networks are separate from each other and also separated from the control and operational technology network. Prevent the use of external hard drives, DVDs and USB memory sticks in the operational and control network.

- **End-user education**

Employees need to understand the risks and instructions for cybersecurity and good cyberhygiene. The entire organization needs to commit and support the agreed policies of safety and security. The program for incident response drills, and general awareness for cybersecurity training, motivating to report cyber-related non-conformities, accidents and incidents, and executing role-specific education, audits and tests. Personnel need to follow compliance regulations and incident management plans need to be tested.

- **Network and physical security**

Define a system inventory diagram for all devices. Restrict logical access to the ICS network with unidirectional gateways, and demilitarized zone (DMZ) network architecture with firewalls and multiple-layer network topology. Disable all the unused ports and services of the devices from the routers and switches. Restriction access to the ICS network and devices with locks, card readers and guards. Keeping firmware up to date increases cybersecurity. Monitor all systems and networks and analyse logs for unusual activity.

- **Recovery and business continuity**

Regular backups of critical information can decrease the time needed for recovery. Duplicating critical and redundant components may prevent and mitigate a cyber-attack.

5 CONCLUSION

This study investigated the question “what to do before risks turn into attacks in maritime cybersecurity”. I used to the following data sources: maritime cybersecurity from authorities, research, university studies, and documentation from ship classification societies. The statistics of cyber-attacks reveal that the rich amount of customer information and financial data makes the maritime industry particularly appealing for cybercriminals.

In order to secure itself from cyber-attacks, all elements of an organisation should understand the needs to understand the threats and risks of cybersecurity that need to be under control and divides into preparedness, situational awareness, prevention, and recovery. The best practices for a successful and holistic cybersecurity program are identifying the organization’s documented IT and OT systems, assets, and people. Critical infrastructure, identity and access control need to be protected before the incident occurs. Personnel training and awareness is essential. A quick reacting to incidents with checklists and containment using response planning process mitigates the event. The incident needs to be resolved in a timely manner. Restoring services with appropriate backups helps to recover the organization to normal operations quicker. Well defined reporting procedures helps organizations learn of the incident and prepare for future incursions.

From the growing statistical trend of increasing cybersecurity attacks in the maritime sector, incidents are likely to grow in the future. Raising and educating awareness in onboard and ashore organisations and infrastructure are some of the main tasks to prevent and mitigate against malware, ransomware, hijacking accounts, system vulnerabilities, DDoS attacks and malicious email spam.

Cybersecurity incidents, service denial attacks and manipulation risk the safety and security onboard vessels. If autonomous and semiautonomous ships, or remotely connected and operated vessels, become commonplace without adequate systematic risk analysis, is there a chance that cyber-attacks risk the safety and security onboard and of the ashore organization? There is a clear need for research on how information and operational technology, and control systems secure to ensure safety on the autonomous or semi-autonomous ship in the future.

Industry 4.0 will affect vessels and the entire supply chain, including the security challenges associated with IoT devices, sensors and communication systems, cloud services, Big Data, and management systems. Cybersecurity needs to take into account every aspect to ensure protection for the personnel, vessels, cargo, logistic chain and systems. These issues need to be studied with precise practice and detailed research to learn how to secure against cyber threats, both now and in the future.

References

Ashton, G. 2020. Maersk, me & notPetya. Available at: https://gvnshtn.com/maersk-me-not-petya/ [Accessed 4 February 2021]

Bimco, Clia, ICS, Intercargo, Intermanager, Intertanko, IUMI, OCIMF and World Shipping Council. 2020. The Guidelines on Cyber Security Onboard Ships, Version 3. PDF document from Bimco. [Accessed 11 January 2021]

Computer Security Resource Center (CSRC). 2021. Definitions in the glossary. Available at: https://csrc.nist.gov/glossary [Accessed 22 January 2021]

Department for Transport. 2017. Code of Practice, Cyber Security for Ships. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf [Accessed 12 January 2021]

DNV GL. 2016. Cyber security resilience management for ships and mobile offshore units in operation. Available at: https://www.dnvgl.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html [Accessed 14 January 2021]

DNV GL. 2020. Maritime cyber security. Available at: https://www.dnvgl.com/maritime/insights/topics/maritime-cyber-security/index.html [Accessed 4 February 2021]

DNV GL. No date. SMS Cyber Security Quick Check. Understanding of maritime cyber risks in light of the ISM Code. Available at: SMS Cyber Security Quick Check - DNV GL [Accessed 5 February 2021]

ENISA, European Union Agency For Network And Information. 2015. Security Definition of Cybersecurity Gaps and overlaps in standardization. ISBN 978-92-9204-155-7. Available at: https://www.enisa.europa.eu/publications/definition-of-cybersecurity [Accessed 22 January 2021].

European Union. 2004. Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0725&from=ES [Accessed 22 January 2021].

Fandino, W. 2019. Formulating a good research question: Pearls and pitfalls. Available at: https://www.researchgate.net/publication/335068238_Formulating_a_good_research_question_Pearls_and_pitfalls/figures?lo=1 [Accessed 27 April 2021].

Interpol. 2020. INTERPOL report shows alarming rate of cyberattacks during COVID-19. Availability at: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 [Accessed 21 June 2021].

Kaspersky. 2020. The state of Industrial Cybersecurity in the era of digitalization. Availability at: https://ics.kaspersky.com/media/Kaspersky_ARC_ICS-2020-Trend-Report.pdf [Accessed 5 February 2021].

Laaksonen, M. 2020. Kyberturvallisuuden trendit 2020-luvulle. Available at: https://dif.fi/blogit/kyberturvallisuuden-trendit-2020-luvulle/ [Accessed 4 February 2021]

Mission Secure. 2020. A Comprehensive Guide to Maritime Cybersecurity. Available at: https://www.missionsecure.com/ [Accessed 11 January 2021]

Nettitude. 2019. Cyber Threat Briefing Considerations for ship owners and operators. Available at: https://cdn2.hubspot.net/hubfs/3021880/M&O_Considerations%20for%20ship%20owners%20and%20operators_Nettitude%202019.pdf [Accessed 11 February 2021]

NIST, National Institute of Standards and Technology. 2015. Special Publication 800-82 Revision 2. Guide to Industrial Control Systems (ICS) Security. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf [Accessed 10 February 2021]

NIST, National Institute of Standards and Technology. 2018. The Five Functions. Available at: https://www.nist.gov/cyberframework/online-learning/five-functions [Accessed 10 February 2021]

NordVPN. 2020. These cybersecurity statistics prove that your security matters. Available at: https://nordvpn.com/fi/blog/cybersecurity-statistics/ [Accessed 25 January 2021].

Passeri, P. 2021. 2020 Cyber Attacks Statistics. Available at: https://www.hackmageddon.com/2021/01/13/2020-cyber-attacks-statistics/. [Accessed 25 January 2021].

Prevailion. No date. Ransomware as a Data Breach Decoy. Available at: https://www.prevailion.com/ransomware-as-a-data-breach-decoy [Accessed 4 February 2021]

Prime Minister's Office. 2019. Government Resolution on Finland's maritime policy guidelines. Available at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161376/VNK%207_19_Government%20Resolution%20on%20Finland%27s%20maritime%20policy%20guidelines_net.pdf?sequence=1&isAllowed=y [Accessed 4 February 2021]

Reuters. 2020. Norwegian cruise liner Hurtigruten sustains cyberattack. Available at: https://www.reuters.com/article/idUSKBN28O1E5 [Accessed 2 February 2021].

ShipTechnology. 2020. Cybersecurity: is the cruise industry prepared? Available at: https://www.ship-technology.com/features/cybersecurity-cruise/ [Accessed 2 February 2021]

Swinhoe, D. 2019. How hackers use ransomware to hide data breaches and other attacks. Available at: https://www.csoonline.com/article/3385520/how-hackers-use-ransomware-to-hide-data-breaches-and-other-attacks.html [Accessed 4 February 2021]

Traficom. 2020. DNV GL Cyber secure class notation. Available at: https://www.traficom.fi/sites/default/files/media/file/5.%20DNV%20GL%20Cyber%20secure%20Class%20Notation%20Information%20Day%20Finland%20handout.pdf [Accessed 10 February 2021]

Tuomala, V. (2020). Logistics and maritime need to focus to cybersecurity in the Internet of Things (IoT) Technology. Xamk Beyond publication. Available at: http://urn.fi/URN:ISBN:978-952-344-279-5 [Accessed 22 January 2021]

Turvallisuuskomitea. 2019. Suomen Kyberturvallisuus-strategia. ISBN: 978-951-663-051-2 pdf. Available at: https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/ [Accessed 22 January 2021]

U.S. Coast Guard. 2019. Cyberattack Impacts MTSA Facility Operations. Available at: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf?ver=2019-12-23-134957-667 [Accessed 5 February 2021]

Walker, J. 2020. AIDA Cruise Ships Under Cyber Attack – Are Costa Ships Also Affected? Available at: https://www.cruiselawnews.com/2020/12/articles/cyber-attacks/aida-cruise-ships-under-cyber-attack-are-costa-ships-also-affected/ [Accessed 2 February 2021]

ACKNOWLEDGEMENTS

Many thanks to Päivi Brunou for evaluating and inspecting my publication, and for encouraging me to move forward in researching maritime cybersecurity.

Thanks are also due to my family and their patience and support, as the whole spring has been devoted to my research and writing.

Vesa

XAMK
RESEARCH

SOUTH-EASTERN FINLAND UNIVERSITY OF APPLIED SCIENCES

1 *Srujal Shah - Kari Dufva:* CFD modeling of airflow in a kitchen environment. Towards improving energy efficiency in buildings. 2017.

2 *Elias Altarriba:* Öljyn leviämisen estimointi arviointitaulukoiden avulla osana operatiivista öljyntorjuntatyötä Saimaalla. 2017.

3 *Elina Havia - Jari Käyhkö (toim.):* Fotoniikkasensori- ja korkean teknologian kuvantamisen demonstrointi metsäbiojalostamon hallintaan (FOKUDEMO). 2017.

4 *Justiina Halonen - Emmi Rantavuo - Elias Altarriba:* Öljyntorjuntakoulutuksen ja -osaamisen nykytila. SCAROIL-hankkeen selvitys öljyntorjunnan koulutustarpeista. 2017.

5 *Veli Liikanen - Arto Pesola:* Physical fun: exercise, social relations and learning in SuperPark. 2018.

6 *Timo Hantunen - Petri Janhunen (toim.):* Sote-alan videoneuvottelujärjestelmien käytettävyys ja käyttöönotto. 2018.

7 *Pekka Turkki:* Selluloosa ja selluloosajohdannaiset elintarvikkeissa. 2018.

8 *Elias Altarriba - Minna Pelkonen - Jukka-Pekka Bergman:* Laadullinen tapaustutkimus opetusresurssien nopean ja voimakkaan vähenemisen vaikutuksista korkeakouluopetukseen. 2018.

9 *Sari Tuuva-Hongisto:* Nuorten syrjäytyminen ja alueellisen eriytymisen vähentäminen. Tutkimuskirjallisuuteen ja –raportteihin pohjautuva kartoitus. 2019.

10 *Susan Eriksson:* Digitalisaatio nuorisotyön opetuksessa. 2019.

11 *Susan Eriksson – Sari Tuuva-Hongisto:* Nuorisotyön digitalisaatio 2030. ”Meidän tulisi osata tarjota nuorille työkaluja maailmaan, jota me emme vielä itse tunne.” 2019.

12 *Susan Eriksson:* Digital applications in youth employment services. 2019.

13 *Hilla Sumanen – Jaakko Harkko – Jouni Lahti – Eeva-Leena Ketonen – Olli Pietiläinen – Anne Kouvonen:* Nuorten työntekijöiden työkyky ja työterveyshuollon palvelujen käyttö. 2020.

14 *Marja Moisala (toim.):* Paikkariippumattomuus nuorten tulevaisuuden palveluissa maaseudulla. 2020.

15 *Hilla Sumanen:* Experiences and impacts of the post critical incident seminar among rescue and emergency medical service personnel. 2020.

16 *Marja-Liisa Neuvonen-Rauhala (ed.).:* XAMK BEYOND 2020. At Your Service – Business Development, Co-operation and Sustainability. 2020.

17 *Mikhail Nemilentsev, Jarmo Kujanpää & Jan Kettula (Eds.):* Research on current and development needs in the automotive and motorsport industry. 2021.