YRKESHÖGSKOLAN NOVIA

Study on cyber security awareness in Finnish ports and shipping companies

Stella Wallenius & Henri Wallenius

Master of Engineering, Autonomous Maritime Operations

Turku 2021

Table of contents

Abbreviations

1 Introduction 1

1.1 Purpose of research 4

1.2 Scope of research 5

1.3 Research problem 7

1.4 Methodology 8

2 Key concepts 12

2.1 Cyber security 12

2.2 Cyber Risk 14

3 Literature review 15

3.1 Regulatory framework 18

3.1.1 IMO regulations 19

3.1.2 EU legislation 25

3.1.3 National legislation 27

3.2 Previous research 27

4 Cyber security and the human element 32

4.1 Human roles within shipping companies 35

4.2 Port-specific roles 37

5 Information Technology, equipment and connections 37

6 Identified cyber risks 42

6.1 Denial of Service (DoS) -attack 43

6.2 Authorization 43

6.3 Social engineering 44

6.4 Data breach 46

6.5 Personal data breach 47

6.6 Malware 47

6.7 Jamming 48

6.8 Malfunction and system anomalies 48

7 Cyber risks: ships 49

8 Cyber risks: ports 54

9 Cyber security management 56

9.1 Identify 58

9.2 Detect 59

9.3 Protect 61

9.4 Response and recovery 63

10 ISM Cyber Security 1.1.2021 64

11 Case study ... 65

11.1 Case study: Ports ... 69

11.2 Case study: Shipping companies ... 70

12 Reflection on research ... 78

13 Recommendations ... 80

13.1 Cyber security in company management ... 81

13.2 Company-specific cyber security training ... 82

13.3 Motivation ... 86

14 Further research ... 87

15 Conclusions ... 88

16 Works cited ... 90

Appendix 1 ...

Appendix 2 ...

Appendix 3 ...

MASTER'S THESIS

Authors: Stella Wallenius, Henri Wallenius

Degree Programme: Autonomous Maritime Operations

Supervisor: Thomas Finne

Title: Study on cyber security awareness in Finnish ports and shipping companies

Date June 2nd, 2021   Number of pages 96   Appendices 3

Abstract

In our study we wanted to find out what the level of cyber security awareness is within Finnish shipping companies and Finnish ports engaged in international trade.

The maritime sector is becoming more digitalized and technological development leads to a higher level of automation. This trend goes hand in hand with cyber security. One of our purposes with this study was to raise the level of security awareness through this study.

The study consisted of literature review, regulatory review and a qualitative research. The qualitative research had two distinct phases, as gathering of data was divided in two parts: material from a cyber security -related workshop for Finnish ports and qualitative interviews with Designated Persons Ashore (DPA's) representing Finnish shipping companies.

Based on our study, training in the field of cyber security is needed. Our view is that we have increased cyber security awareness by raising the issue and encouraging discussion. Currently the shipping companies are implementing ISM guidelines on cyber security so the timing was suitable. Cyber security should be included in the risk management process.

Language: English

Keywords: cyber security, digitalization, interconnectedness, security awareness, human behaviour, risk management, ports, shipping companies

Abbreviations

ACL	Access Control List
AIS	Automatic Identification System
ANSSI	Agence nationale de la sécurité des systèmes d’information
ARPA	Automatic Radar Plotting Aid
BIMCO	Baltic and International Maritime Council
BYOD	Bring Your Own Device
CEO	Chief Executive Officer
CLIA	Cruise Lines International Association
COVID-19	Coronavirus disease 2019
CSO	Company Security Officer
DoS	Denial of Service
DPA	Designated Person Ashore
DSC	Digital Selective Call
ECDIS	Electronic Chart Display and Information System
EMSA	European Maritime Safety Agency
ENISA	European Union Agency for Cybersecurity
EPFS	Electronic Position Fixing System
EPIRB	Emergency Position Indicating Radio Beacon
EU	European Union
GDPR	General Data Protection Regulation
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positioning System
HCI	Human-computer interaction
HCS	Heading Control System
HR	Human Resources
ICS	International Chamber of Shipping
ICT	Information and Communication Technology

IMCO	Inter-Governmental Maritime Consultative Organization
IMO	International Maritime Organisation
IMSO	International Mobile Satellite Organisation
INS	Integrated Navigation System
IP	Internet Protocol
ISM	International Safety Management
ISPS	International Ship and Port Facility Security
IT	Information Technology
MARPOL	International Convention for the Prevention of Pollution from Ships
MLC	Maritime Labour Convention
NAVTEX	Navigational Text Messages
NCSC	National Cyber Security Centre
OT	Operation Technology
Radar	Radio Detection and Ranging
SART	Search and Rescue Transponder
SDME	Speed and Distance Measuring Device
SOLAS	International Convention for the Safety of Life at Sea
SSP	Ship Security Plan
STCW	International Convention on Standards of Training, Certification and Watchkeeping
TCS	Track Control System
USB	Universal Serial Bus
USCG	United States Coast Guard
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WMU	World Maritime University

1 Introduction

We live in a highly information-dependent society. Many functions in our society have become more digitalized and interconnected as a result of general technical development. The shipping industry and port operations are following this same trend. This means that more processes are digitalized and take place online. The need to protect these processes and ourselves from e.g. cyber-attacks, human errors as well as technical mistakes, 'bugs', have become increasingly important issue.

The exchange of information within shipping operations involves many different actors. The logistical exchange is complex, consisting of shipping company, charterer, ports, agencies, technical management, subcontractors, supply deliveries to the ship etc. Time is money and unnecessary waiting time in ports or anchorages is to be avoided in every possible way. There are challenges in keeping the processes smooth with no delays. It is also challenging to manage all the needed check-ups and procedures with various actors in the ports smoothly. The information moving between all actors involved must be transferred without interference.

Benefits from better and more efficient processes for transmission of information are evident in various processes within the shipping operations. Functions related to human resources, such as accounting, payroll and recruitment can nowadays be handled by smaller departments due to advanced technology and information systems. Communication between shipboard crew and office workers is better and more frequent. Operators involved in the cargo supply chain such as cargo owners, operators, agents and authorities, have easier ways to locate and contact each other. (McNicholas, 2007, 367)

A clear change is seen for example in the decision-making process on-board a ship's bridge. Where in the past one would rely solely on observations, knowledge and even sense, there is today so much more data to handle in lieu of experience and knowledge. The development naturally strives for increased safety on-board and is supposed to assist navigators, but on the other hand we stumble on new risks. (Fitton et al., 2015, 4)

Technical development seems to be continuing with a great pace. Often commercial interests are the driving force; how much can we limit access and transmission of data in a world where things "need to be done yesterday"? There is a clear need for a proper balance and this means risk management. Before the modern day advancements in communication technology, when connectivity and transmission of data between ships and shore were not possible, the ships were out of reach and isolated. Now ships and their crews are on-line to a larger extent and everywhere (Fitton et al., 2015, 2-3). In this new environment we face new kinds of threats and challenges to ships, ports and shipping operations.

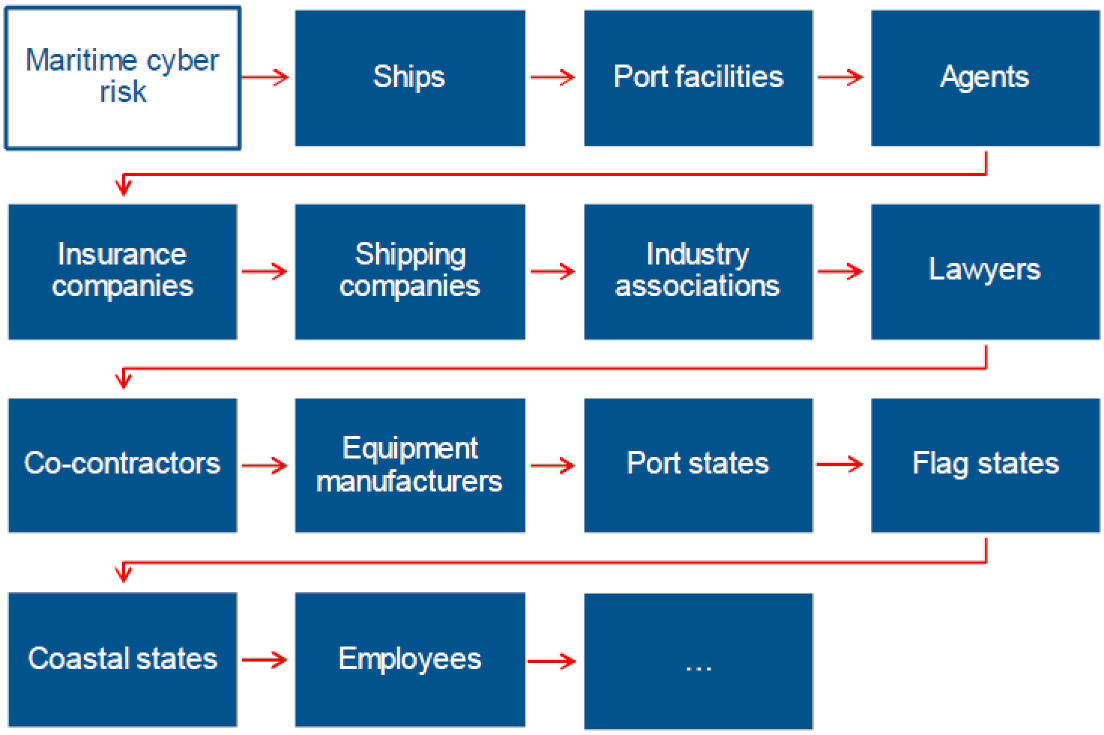


Figure 1. From presentation by Dr. Liliane Rossbach at EMSA, Workshop "Cyber-Attack Prevention” 13 - 14 December 2017 – EMSA, Lisbon Portugal

The general view which we have encountered several times in different forums and discussions, is that the cyber security awareness is not at an adequate level. The starting point and research problem of this thesis is to look more thoroughly into this with a scientific approach. We strive to solve the general level of cyber security awareness within the Finnish maritime industry. By maritime industry in this context we mean commercial shipping and related port operations. We focus on ports and shipping companies and we decided to do a qualitative study. Ports and shipping companies represent the core of the maritime logistic chain.

Fitton et al. (2015, 21) suggest that since shipboard life always has emphasized safety on-board, because the crew is so far away from getting assistance, the focus on online safety training should be included in that entity. How will shipping companies in Finland see this issue? Do the increased amount of technology, connectivity, information and data transmission cause a cyber risk which requires the same level of safety measures and defined processes as the traditional risks and preparedness for emergencies on-board?

In this thesis, we want to examine the human element, not so much the technical solutions, in the cyber security context. The main goal of the study is to find out the current level of knowledge and understanding of cyber security within the defined scope. The scope of the study is opened in more detail under subtitle 1.2. We also want to identify the critical weak points in cyber security related to the human factor and the kind of threats people, in different roles, can cause.

The human element can be divided into *intentional acting* with the aim to achieve own interests and *unintentional errors*, which are causing damage (McNicholas, 2007, 374-375). To conclude why we want to look at the human element's role as within cyber security we want to quote Fitton et al. (2015, 15):

> "Even in the most secure computer systems there is a vulnerability which cannot be patched, corrected or rewritten. The human being is highly fallible and easily manipulated. They are also capable of free and critical thoughts which might lead them to breach security procedures or break the law in the name of their cause".

This cartoon well illustrates the quote above:

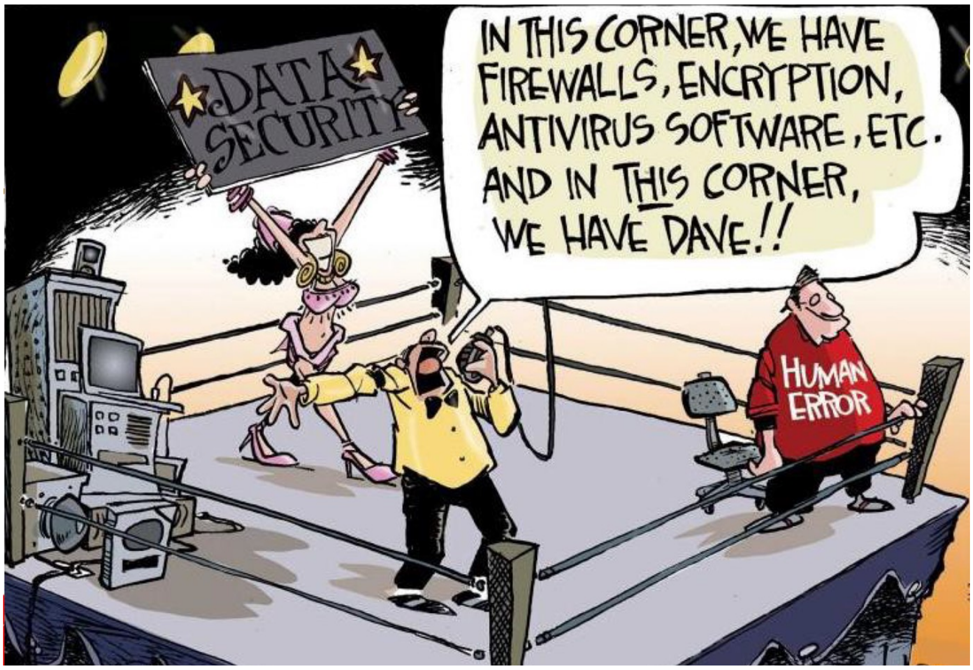

DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

Figure 2. Cartoon by John Klossner

1.1 Purpose of research

The human factor plays a major role either directly or indirectly in the vast majority of accidents and mishaps. Therefore, one must logically conclude that the level of competence and level of human awareness must be in a key role also in cyber security-related threats. A USCG report states that between 75–96% of marine casualties are caused at least partly by some form of human error (Rothblum, 2000, 13-20). This report is more than 20 years old but it is still used as a general reference within the maritime domain.

Voeller (2014, 41) mentions the term HCI – human-computer interaction – and states that

> "the "human element" is a critical component of security, and that it is possible, with care, to build systems that are both usable and secure."

Maritime operations may suffer from major economic and environmental damage if something goes wrong. The employee's understanding of cyber security is already, and will be even more so in the future, of utmost importance in order to guarantee safe and secure operations within the maritime industry.

Learning by mistakes is something familiar to us all. We suffer from limited resources in today's information-based, connected and highly technologized world. Things must be done fast, including sending-receiving information and making decisions based on it. The maritime industry has traditionally been considered to be an old-fashioned field of business with traditional and manual processes. Nowadays it is a part of the digitalized and connected world. The increase of technology usually means more tasks to be handled by fewer hands and heads. How can the maritime industry prepare and protect itself from information technology malfunctions, data breaches and attacks within an appropriate period of time, with limited financial resources and energy? What is there to be done in order to be better prepared and protected and hopefully decrease the risks without having gone through several mistakes first?

It is of crucial importance for people who operate in this safety-critical work environment to have knowledge of the cyber risks associated with these operations. By informing the users some of the threats can be decreased. Even the best technical solutions can be compromised by intentional, neglectful or ignorant human behaviour. There is no firewall which could prevent for example an employee from giving their credentials to a hacker (Jaf et al., 2018, 4989).

This study aims to find out the general level of knowledge about cyber risks and the preparedness against them. In addition, the aim of the study is to increase the cyber security awareness and to disseminate best practices.

1.2 Scope of research

The globally running maritime industry includes a large variety of operators, vessel types and sizes. As in everything else in society, the level of technology and digitalization varies a lot from one country, port and shipping company to another operator in another part of the world. Below two pictures visualizing the difference:

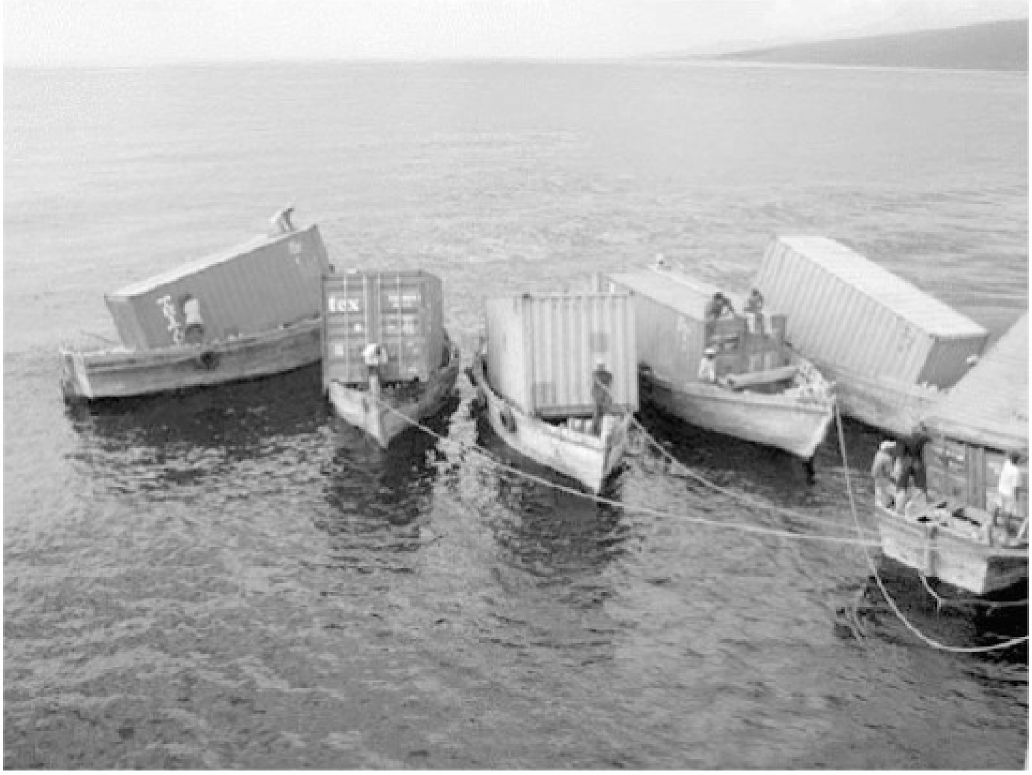


Figure 3. Container ships fully loaded. The level of automation in this port is unlikely to be very high (McNicholas, 2007, 25)

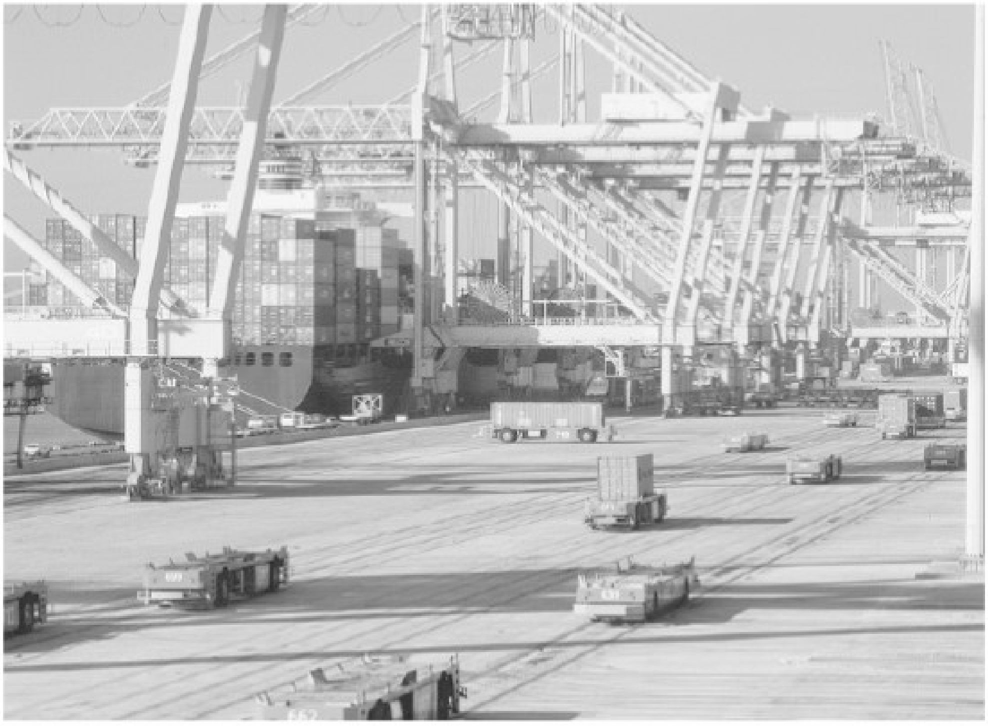


Figure 4. Unmanned vehicles shifting containers in a highly automated port (McNicholas, 2007, 12)

We have limited our study to the situation within Finnish shipping companies and port operators. Statistics from 2019 show that we in Finland had 116 merchant ships in international trade. In August 2020 the number was 113 and in April 2021 115, so the number has remained about the same. (Statistics Finland) The official statistics show that the number of ports with international trade in Finland was 48 in year 2017. Regarding shipping companies we used the Finnish Shipowner's Association as a source, and can see that in October 2020 the association had 23 members. To summarize the maritime sector of shipping companies, ships and ports involved in international trade in Finland:

- Shipping companies 23 (2020)
- Ships 115 (2021)
- Ports 48 (2017)

Of these we chose five different shipping companies of different sizes and with different vessel types. For the part covering ports we used material from a workshop arranged by Traficom in 2019. This will be further clarified in the methodology chapter.

We realize that shipping companies and ports are reserved when sharing information regarding safety and security. In order to achieve as much information as possible, we will not describe the subjects of this study; e.g. not mention types of vessels or the individual companies and ports. The purpose of this research is to make general findings throughout the industry and not to focus on certain operators or define different risks for different sizes and types of vessels or ports. In addition the Finnish maritime cluster is rather small and specific ships or companies will easily be identified if categorized.

When specifying the role of the human element we have decided to exclude threats from inside of the company, which would require another framework and point of view. This would be connected to recruitment, follow-up and control of workers. We think that risks involving deliberate actions from the company's own workers would probably include also other risks than cyber security breaches, which we want to focus on. These other threats can be e.g. theft or distributing sensitive data about the company, which not necessarily is stored and distributed via digital means. The level of background investigations when recruiting is a sensitive issue in Finland, where the data protection regulations are strict.

Fitton et al. (2015, 16-17) mention the use of social media, including contacts. Such information can enable stealing a seafarer's identity and information from the social network can be used as blackmail. Being far away from home with no or limited contact, the seafarer can be an easier target. These kinds of cyber security risks or attacks, where the channel is via the seafarers' contacts, are not in our scope.

Last but definitely not least, there might be cyber-attacks, deliberately caused by humans but to such an extent that a private-owned shipping company nor a port in a small country like Finland, could possibly foresee it. A new field of security, or the absence of it, can attract even nations to cause an attack. This kind of cyber-warfare would cause damage to nation-wide operations and digital infrastructure and networks (Sales, 2013, 1504-1507). We decided to exclude this kind of high level cyber-attacks, which are difficult or impossible to predict.

1.3 Research problem

We want to study the level of understanding of cyber security and -related issues among Finnish shipping companies and ports. We are interested in whether improvements are needed and if we can make conclusions and disseminate good practises by this thesis, to the industry. In any case, raising these issues is already a step in the right direction.

Our research problem can be defined as:

What is the level of cyber security awareness among Finnish shipping companies and ports? Have cyber security incidents, data breaches or malfunctions occurred? Furthermore: can we identify areas for improvement?

1.4 Methodology

The study consists of literature review, short regulatory review and a qualitative research. The qualitative research consists of two parts:

1. Material from a cyber-security workshop arranged on April 9th 2019. This workshop was arranged in collaboration by Traficom, Suomen Satamaliitto ry, Satamaoperaattorit ry and Hazard-initiative. The workshop was arranged for port operators and other key players in the ports. This workshop gave us a good contribution to the research problem concerning ports. We also added some findings from an ENISA report (Drougkas et al., 2019)

2. Interviews with five shipping companies engaged in international trade

Walliman (2010) describes research methods from different views and one aspect is the design of a research, which leads the project towards a certain choice of method. The research method follows a descriptive design, where we observe and collect data and analyse it in order to understand the situation. (Walliman, 2010,9-10) When deciding how to collect the primary data for this particular research, we find it obvious that we will not solve our research problem through a quantitative study where the data are presented in numbers via statistical methods. The scope is too small and heterogeneous and the questions to be answered (what / where / how) too complex. Furthermore, the research question will to some extent be related to the interviewees' beliefs and/or attitudes, which have to be analysed in words and not in numbers. (Walliman 2010, 71-72)

There is a challenge when making notes from interviews; answers may be simplified and some personal interpretations are being made during the process of sampling and analysing the collected data. Our field of research includes sensitive data about the targets' cyber security -related awareness and experience. The information must naturally be presented in a way which guarantees anonymity and this must be also communicated to the interviewees. (Walliman, 2010, 48-49)

A previous study on cyberattacks, conducted by sending questionnaires to shipping companies and maritime administrations, did not succeed in gathering information. In this study answers received were: shipping companies 16 sent, 2 received and maritime administrations 14 sent, 3 received. One reason for the low participation is the sensitive information involved (Silgado, 2018).

Sending out a questionnaire as such would require a large number of recipients because people tend not to bother answering. The maritime industry in Finland, which we decided to define as the scope in this study, does have a very limited number of shipping companies and ports. It was evident from the beginning that even if we would include all of them, the chance to get a sufficient response rate would be unlikely. Also Walliman recognizes the uncertainty related to getting replies from questionnaires, either sent by traditional mail or e-mail (Walliman, 2010, 97). Furthermore, the quality of the answers tends to be bad, as the questionnaire may not seem important to the respondents which decided to answer and they want to get it over with as soon as possible (Gillham, 2007, 9). We have personal experiences of questionnaires, where there are reminder-e-mails sent out and then finally one decides to contribute but not with the best effort or thought behind every answer. The answering options may not be suitable and then you simply choose the option “I don’t know”, “I do not have experience on this” or you tick the average number on a scale of 1-5.

Even though our field of research is fairly limited, we will not cover the whole Finnish maritime industry but choose a few. How then to choose the most appropriate sample of those 23 shipping companies and 48 ports engaged in international trade? Walliman (2010, 93-94) talks about case studies when using only a few subjects for a more detailed survey. One can also use different types of subjects in the scope and analyse that material, as a comparative approach. (Walliman, 2010, 93-94)

After having reviewed different options for gaining primary data for the study we decided to apply a qualitative survey with five shipping companies engaged in international trade. The material regarding ports is based on the workshop mentioned earlier. This workshop covered Finnish port activities quite well, with 43 participants from different port related companies and authorities. The maritime industry in Finland is rather small. We can contact the subjects directly, discuss our study, and explain how we will use the data. Since we will have only a few subjects for our research, it will be formed as a case study. We can compare the results or make conclusions, depending on the outcome. Information for the case study will be collected by interviews (ships) and by using the workshop material (ports), as stated earlier. We should note the challenge of what our respondents believe and what they actually do and how to "double-check" their beliefs. Collecting data from several sources is preferable. (Gillham, 2000a, 13-14). If the answer is "Our staff is well-trained in cyber-security related issues" and no evidence of this is found, such as documentation in the company's ISM-manual, we must dig deeper. Moreover, even if people know cyber-security to be a risk, they might not act on it. We think that during an interview, when discussing freely, the respondents are more likely to explain their answers than in a questionnaire where simply stating "yes" or "no". We can also immediately interact if we realize a question is tricky or does not provide added value to the study.

Focus must be on forming the questions. What information do we need in order to answer the research questions? When forming them we can reflect on how we would answer those questions (Gillham, 2000a, 17).

The format of the interview will be semi-structured, which can be seen as the most important research method in a case study (Gillham, 2000a, 65). Some information we need from all respondents in a standardized format and some will be open and we will be prepared for additional questions in order to gain information of value to this study. During an interview we can also rephrase questions, repeat them and explain to make sure the questions are understood. Interviews can be conducted in different ways and for us the only option in the time of COVID-19 -pandemic is by telephone or online meeting application like Skype or Teams. This also makes the survey-process more efficient and geographical factors will not have an impact on the sample. All of the interviewees will be treated equally, which gives an objective base compared to conducting some of the interviews face-to-face by meeting at their office and some by telephone. Collecting facts from different sources, such as observations in the working environment, hearing and seeing people in their work, is left out from this remotely conducted interview. However, as we are collecting data we may add respondents to our list and thus expand the sources of data. This is often reality when doing research that both questions and the collecting of data develop as the project goes on. (Gillham, 2000a, 16-17, 22-23). In our case we were satisfied with the original plan and scope of targets for collecting data. The type of answers were quite similar. No major deviations were found, which may have resulted in the need to dig more in order to find a general view, which was the aim of this study.

Telephone interviews are more successful when the interviewer knows the subject, when you can explain what the survey is about and schedule the interview for a suitable time (Gillham, 2000a, 77). In our case it may not be 100% true for all subjects but for some of them and the rest we will probably have an indirect connection to. As said earlier, the industry is small and we have both been working in the maritime sector for more than 20 years. We feel confident about getting the remote interviews booked. The COVID-19 pandemic has resulted in working from home and many conferences and scheduled appointments have either been cancelled or moved on-line. This means that office workers have saved time when not travelling to workplaces or other locations for different events. Our interviewees are thus used to meeting on-line and cooperating without meeting in person. We believe this is an advantage for us.

An interview is a situation where the subject is in focus. This is one reason why people rather answer questions orally than answering a questionnaire. Another is that it is easier than writing, especially when open questions occur. (Gillham, 2007, 7-8, 14-15)

Analysing the material from interviews can be very time-consuming. According to some experts the only way to collect the data is recording and transcribing (Gillham, 2007, 9-10). Transcribing the conversations would ensure the recording and analysis of exactly what was said, but since the time is not unlimited for us we will make notes. As the analysing of data often is a very complex process in qualitative studies, we realize that as much information, comments and remarks as possible shall be documented during the interviews (Walliman, 2010, 99-100, 131).

The disadvantage when taking notes versus recording the interview is clear: some parts may not be quoted as they were said and some personal interpretations may occur (Gillham, 2000a, 66-67). Listening to the answers, trying to focus on the interviewee and making notes at the same time can understandably be a challenge. Either the subject of the interview does not feel he/she is being listened to, it is difficult to fluently find an appropriate response or sub-question or the notes suffer. Since we are two persons conducting this study, one of us will ask the questions and have constant focus on the Interviewee and the other one can concentrate on writing down as much as possible. We will have a double set of ears listening and brains analysing the data afterwards.

2 Key concepts

During our studies within the programme on autonomous maritime operations we have stumbled on the challenge with definitions several times. New technologies, new risks and unclear definitions tend to go hand in hand. The context in which terms are being used has a major impact on the definition. Therefore the first step in order to make a study is to define the concepts in order to have the same understanding throughout the project; the authors when planning the qualitative research and making analysis and the interviews when answering questions. In our work the most relevant and important terms are "cyber security" and "cyber risk". What do they mean in this context? Most challenging and for the maritime industry also threatening, are the risks yet fully identified. How can we prepare ourselves for what we do not know or understand?

Furthermore during this work we also found terms such as computer security, hardware and software security, internet and network, application and database security (McNicholas, 2007, 371-374). These kinds of divisions might confuse the subject for our field study even more so we must use a more general definition.

We aim to describe possible risks for the maritime industry. We will not use the familiar tool when making risk assessments which is grading them; which is more likely and causes most harm and where is the likelihood smaller. Shipping companies, their ships and the port systems are so different and the risk management should of course focus on that particular business. The organizations should point their resources at identified high-risk areas, critical functions and systems. This can mean a risk which is likely to occur and causes damage to the business and is different for different ship types and sizes.

Here we have defined the recognized key words "cyber security" and "cyber risk" at a general level.

2.1 Cyber security

Security as such was introduced to the maritime sector and included in regulations, certificates and training requirements as a consequence of the World Trade Center terrorist attacks as late as 2001 (McNicholas, 2007, 89). A new code was created as a mandatory set of regulations to protect human lives, the environment and property against security threats (IMO, 2020). The code does not clearly highlight cyber security, but it can be interpreted to be included in the code through threat identification and preparedness. The code will be clarified later in chapter 3.1.1.

One obvious source from which to seek a commonly used definition for cyber security for ships is the International Maritime Organization. The IMO is the fundamental base for maritime regulations, recommendations, training and certification requirements for ships, their construction, machinery, equipment, processes and people involved. However, at the time of writing, no new mandatory, cyber security specific legal instruments have been implemented. We know the regulative process is slow and that the maritime industry itself has acknowledged the need to be protected from cyber threats. We also are aware of the fact that technology has evolved faster than the requirements, so we will also look at some well-known manufacturers and other actors, such as classification societies', suggestions for definitions. We find that for us to achieve the most suitable definition, we will start by quoting our sources and at the end of this chapter conclude the one to be used in this study.

- International Maritime Organization (IMO)

  The IMO has published a 12-pages long table with different cyber-related terms:

  > "Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."

- Gard - the well-known insurance company within the maritime sector explains:

  > "Cyber security, also known as computer security or IT security, is the protection of information systems from theft of or damage to:
  > • the hardware
  > • the software
  > • the information contained in the systems and disruption or misdirection of the services they provide." (Gard, 2017, 3)

- Wikipedia

We wanted to also mention the Wikipedia definition, since it is the largest and most up-to-date encyclopedia, even for scientific use. (Wilson & Likens, 2015, 1). When using the search word "cyber security" it automatically changes the result to "Computer security". Maybe because it is a more down-to-earth term? However, according to Wikipedia, cyber security (computer security) means:

> “Computer security, cyber security or information technology security (IT security) is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.” (Wikipedia, 2020)

- BIMCO, CLIA et al. (2017) have published a generally used cyber-security document within the maritime sector is ”The Guidelines on Cyber Security on-board Ships”. Even the IMO refers this document in its own guidelines. The guidelines describe as follows:

> ”Cyber security is concerned with the protection of IT (information technology), OT (operational technology) and data from unauthorised access, manipulation and disruption.”

After having reviewed some definitions for the term cyber security, our conclusion for the purpose of this study, where we have the human element in focus, is:

“Cyber security means protection of data, technological instruments and assets. It includes the human element, the users of the information, technology and applications and networks. The humans can be tricked or manipulated in different ways and on the other hand, they can be the heroes when protecting their ship(s) and company from disaster or minimizing consequences”

Jaf et al. (2018, 4988-4989) bring up the term “social engineering” in the context of cyber security, even though one could argue that it belongs under “security”. This means manipulating a direct contact – a person – in order to obtain access to inside an office, which requires authentication, or via blackmail retrieving classified documents for their own benefits. We will include this in our study. The assumption is that due to familiar security trainings for both ships and ports, the sectors are already cautious regarding allowing physical access through port gates and to office building, let al.one on-board, without having checked authorization.

2.2 Cyber Risk

The IMO explains the term maritime cyber risk as:

> ”a measure of the extent to which a technology asset could be 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.” (IMO, 2021)

This is interesting, since "technology asset" is formed as a condition which needs to be fulfilled in order for the risk to be defined as a "cyber risk". During this study we have come across the belief that cyber security would also cover *information* and not necessarily require the "technology asset". Here is a link towards the term "social engineering", which we include in the concept of cyber security. We will get back to social engineering later in this study and summarize "cyber risk" as:

"an unwanted incident, deliberately caused or by unintentional error, which may cause damage or malfunction to a company's information technology systems, networks or cause data breach."

3 Literature review

Cyber security, covering issues related to information technology, connectivity and networks, is a rather new phenomenon which means it evolves at a high speed. We realized that in order to retrieve as much updated information as possible, we would mainly rely on e-books and articles from scientific journals in our background search; databases EBSCOhost and ProQuest. Google Scholar helped us to find more recent material and we went through also some non-academical sources and articles found in the internet to get a wider picture of the current situation.

A study on how to measure the status of cyber security within a company has been done by Voeller (2014). It is a collection of several authors' work and the main focus is on technical solutions and how to find the weaknesses and strengths in computers, firewalls, anti-virus software etc. There are parts which include the human element such as knowledge of anti-virus-systems, encrypting e-mails and security of passwords. Since we in our study want to focus on processes and human factor, we decided to use those relevant segments from this particular source as a framework.

Cyber risks in general are presented by Ulsch (2014). He reflects on what issues lie behind and which circumstances create the threats to a company. United States' security and terrorists are a point of focus in the study. A general reflection is that the importance of cyber security threats has not gained the focus it should in different organizations, especially among management. This is a general work of theory from where we can identify threats. However, the maritime industry has its special features in relation to land-based organizations. Ships and ports today rely on information exchange for maximum effectivity and optimization of processes. On the other hand ships at sea might be disconnected and out of reach. Furthermore, the business is very global which means the differences between the levels of technologies are huge. Cyber-attacks conducted by terrorists, would aim for causing deaths, damage to a large part of society or financial gain. Terrorists would want to attack critical infrastructure of a society (Ulsch, 2014, 58). Our opinion is that a small maritime industry in the north far away from oceans, such as Finland, would *in general* not be of high-level interest to terrorists or targeted cyber-attacks. Naturally size and type of ships (passenger-cargo), value of cargo or the ship itself (tanker-icebreaker) and other factors have an impact on the level of interest for harmful actions classified as terrorism.

McNicholas (2007, 376) has found risks within information security, such as information in the wrong hands. This could happen due to hackers but also human errors. Office-workers today are under pressure. The e-mail traffic is frequent and the expected response time is short. The risk of human element causing cyber security -related problems has been found evident and the authors of this study have ourselves experienced that auto-filling of recipients' e-mail addresses has resulted in the wrong address and that has not been discovered before clicking "send". Often these kinds of human errors are innocent incidents, but with bad luck classified and even harmful material can reach an inappropriate contact.

Keeping our work on laptops and keeping the laptops with us has been more common as technology has evolved; the laptops become smaller and Wi-Fi connections better. We work from public transport, hotel lobbies and from home. This means that we carry sensitive material with us with the risk of it getting stolen. One risk is that getting in the wrong hands, the information can be obtained and used for intentional bad purposes. The other, also mentioned by McNicholas (2007, 368), is that important information to the company might be lost and never found if stored on the hardware. However, today due to the good connectivity, much information is stored in clouds and servers and people acknowledge the importance of backups.

Further on, McNicholas (2007, 370-371) finds five key objectives related to information technology security:

1. Confidentiality

    - Data only accessed by authorized persons

   - Measures of protection: firewalls, antivirus systems
   - Requirements from e.g. GDPR (European Union)

2. Integrity
   - Quality of data
   - Measures of protection: different edit checks

3. Availability
   - Decisions depend on updated information in a 24h business such as the maritime industry
   - Measures of ensuring: backup, remote storage networks, recovery programs

4. Nonrepudiation
   - Verification of designated persons before granting access
   - Measures of ensuring: digital signatures (versus paper-pen signature, which is easier to forge)

5. Authentication
   - Verifying the identity of designated persons with access to the specific information
   - Measures: user ID's, passwords, biometric systems

Regarding the work on the bridge, where most of the crucial information technology on-board of the ship is situated, the International Chamber of Shipping has published a Bridge Procedures Guide. The best practices for work on the bridge includes one paragraph covering cyber security. It recognizes risks related to the users, such as updating navigational systems. Furthermore, it refers to existing regulations and guidelines and company-specific procedures. (ICS, 2016, 59)

Chistopher Hadnagy (2014, xxi) begins one of his books with the words of encouragement that that particular book can be of assistance it "battling the cyber war".

The book covers social engineering so we used this as a base when looking into that kind of cyber security threats.

Moving forward to managing the cyber risks, Salmon et al. (2017) have presented network risks and related protective measures. This is also a general view on the subject and included technical instructions on how to perform different security checks. We chose short, relevant parts without going too deep into technical issues.

Cyber security from a shipping company's point of view is not limited to work at an office or on-board a ship. It is also related to private use of different mobile devices, especially when connecting them to company wireless networks. We found a recently published hands-on-approach regarding these risks written by McDonough (2019). This piece of work we found to be very useful – it is not outdated and not too technical. It is aimed at average users which our target group represent and especially on-board ships private use is a means of recreation for the crew. In fact, the International Maritime Organization encourages shipping companies to provide for internet access for its shipboard personnel. Internet usage can be assumed to occur also among employees in ports, during breaks and waiting times etc. Not only can the private use cause damages to company networks and further on to equipment, but it is noteworthy that if employees learn to protect their private networks, devices and e-mail accounts, it is likely that their best practices will transfer to the work environment, too. From this book one could use down-to-earth explanations to implement in a company-specific cyber security awareness-program, if needed. Furthermore, if employees receive valuable information that can help them from being scammed in their private life, the training in itself can be more effective and the participants more receptive!

3.1 Regulatory framework

The regulatory framework consists of both international and national aspects, as always in the international maritime context. It is noteworthy that there are no cyber security specific legal instruments in force at the time of writing, only recommendations and other maritime security regulations that are mainly created the physical security in focus. The latter, of course, refers to the SOLAS chapter XI-2 and the ISPS Code.

In this part, we give a view to the legal framework concerning maritime operations. Since the maritime industry is regulated on different levels, we will look at both international, European and national regulations. This overlook will touch lightly on the most important maritime legal instruments and recommendations and cannot be considered as all-inclusive. Some regulations may be stricter within EU-area and this should be taking into account when making contracts with service providers or suppliers or outsourcing processes.

3.1.1 IMO regulations

The International Maritime Organization has the most important role when it comes to regulations concerning shipping. It is worth to mention a few words about the IMO's background here and to bring forth a few of its key legal instruments.

The International Maritime Organization is an agency of the United Nations.

> "IMO is the global standard-setting authority for the safety, security and environmental performance of international shipping. Its main role is to create a regulatory framework for the shipping industry that is fair and effective, universally adopted and universally implemented" (IMO introduction, 2018).

IMO was formally established in 1948 in Geneva conference. The original name of IMO was the Inter-Governmental Maritime Consultative Organization, or IMCO, but the name was changed in 1982 to IMO. The IMO Convention entered into force in 1958 and the new Organization met for the first time the following year.

The four pillars of international maritime law are familiar to most people involved in seafaring and often mentioned as the most fundamental maritime regulations. Three of these pillars are IMO regulations, which SOLAS Convention, MARPOL Convention and STCW Convention. The fourth is MLC (Maritime Labour Convention), a convention by the International Labour Organization. The MLC includes human security, such as social, financial and health protection. Among other it sets minimum standards for living conditions on-board and recreational facilities. The MLC, as most other maritime conventions, consists of mandatory regulations and recommended guidelines. Each regulation is connected with a relevant recommendation. Regulation 3.1 covers the recreational facilities, which is relevant here. The mandatory part does not set detailed descriptions on what kind of entertainment must be available, it only states that there shall be "appropriate recreational facilities, amenities and services" for all seafarers and further refers to respective guidelines. The guidelines include a recommendation for arranging access to the Internet and e-mail. If charging the seafarers, it should be set to a reasonable amount.

The work related to developing global legal framework is a complicated and time-consuming process. Cyber security is a field with rapid development, which makes it difficult to achieve successful results. The situation is not made easier by the fact that IMO's main focus is at sea, but the ships also enter ports and ports are largely outside of the scope of IMO regulations. Ships are expected to operate for approximately 25 years. They are sold and bought during this time and investments may be set to minimum, which can result in outdated anti-virus and other protective systems. Old technology has been used and designed before cyber-attacks were an issue to keep in mind when building the system. (Hopcraft & Martin, 2018, 3).

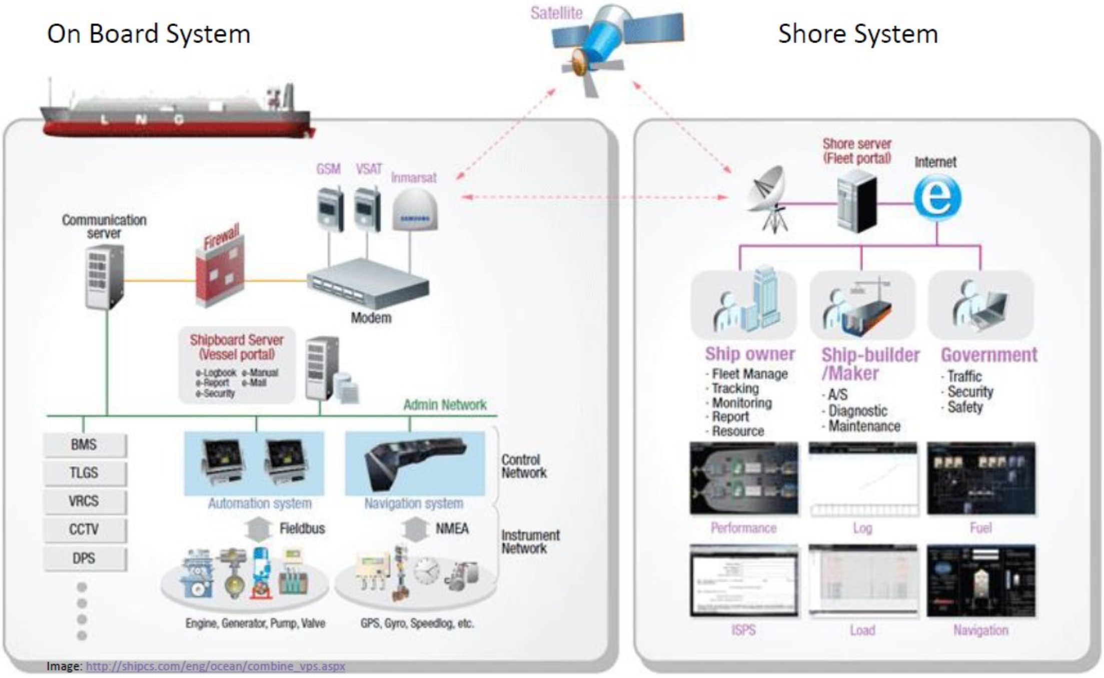
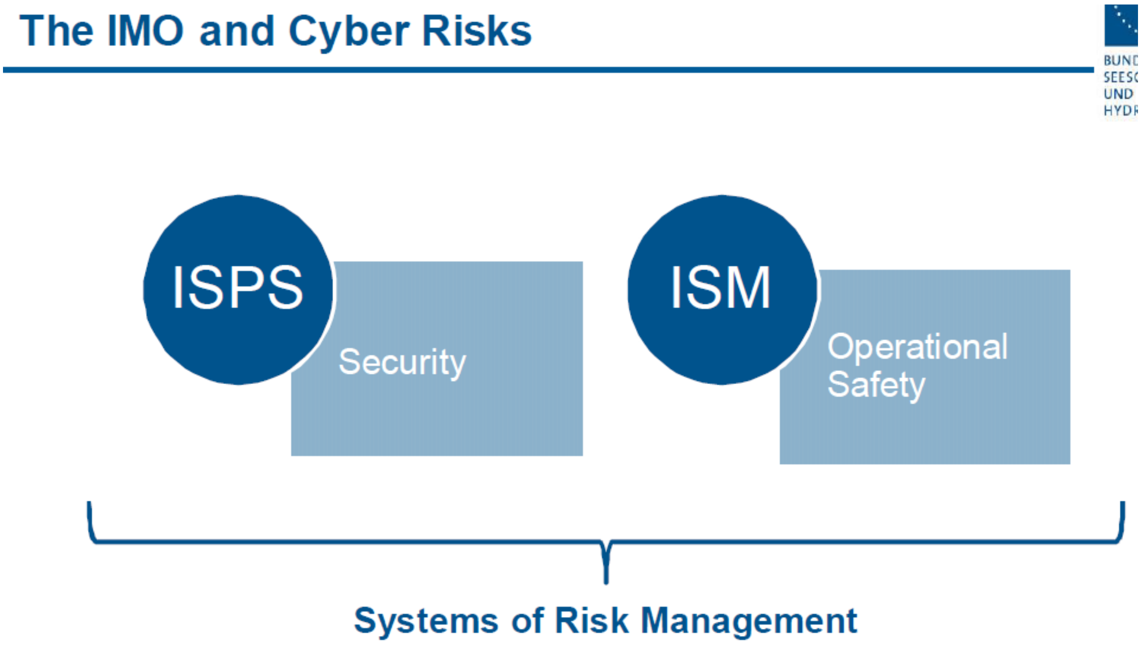


Image: http://shipcs.com/eng/ocean/combine_vps.aspx

Figure 5. On board systems and Shore systems, Presentation by EMSA, 6.3.2019 Maritime Cyber security Table Top Exercise, European Maritime Safety Agency's (EMSA)

SOLAS, the International Convention for the Safety of Life at Sea, is an international maritime treaty, which sets minimum safety standards in the construction, equipment and operation of merchant ships. The convention requires signatory flag states to ensure that ships flagged by them comply with at least these standards. The current version of SOLAS is the 1974 version, known as SOLAS 1974. SOLAS is generally regarded as the most important of all international treaties concerning the safety of merchant ships and it is regularly amended with new provisions. (IMO SOLAS Convention)



The IMO and Cyber Risks

ISPS

Security

ISM

Operational Safety

Systems of Risk Management

Figure 6. From presentation by Dr. Liliane Rossbach at EMSA, Workshop "Cyber-Attack Prevention" 13 - 14 December 2017 – EMSA, Lisbon Portugal

The following paragraphs in this chapter, concerning the ISPS Code (International Ship and Port Facility Code) and the ISM Code (The International Safety Management Code), are based on the authors' experience and knowledge of the subject matter as well as on some presentation materials of authority meetings which are not publicly available. One of the authors (Henri Wallenius) has been involved in maritime security for several years. The experience includes different positions within the maritime authority since 2005 and Henri acted as the national ISPS focal point between 2015 and 2020. The role as ISPS focal point is defined in the Regulation (EC) No 725/2004, Article 9, paragraph 2.

As shown in figure 6, the two key legal instruments for risk management of the IMO are the ISPS Code and the ISM Code.

SOLAS chapter XI-2 and the ISPS Code have been in force since 19th May 2004. Chapter XI-2 and the ISPS Code regulate and also bring special measures to enhance maritime security in many ways. The main focus in these regulations are in physical security and access control as well as establishing roles and responsibilities. The ISPS Code applies to both ships and ports.

The ISPS Code is divided into two sections: Part A and Part B. Part A, which is mandatory, includes the maritime and port security related requirements which shall be followed by the governments, port authorities and shipping companies. Part B provides guidelines on how to meet these requirements. The main objectives of the ISPS Code include detection and deterrence of security threats, establishment of roles and responsibilities, collection and exchange of security information, providing a methodology for assessing security and means to ensure that adequate security measures are in place.

As mentioned previously in chapter 3.1, the ISPS Code does not specifically highlight cyber security, but it can be interpreted that at least following parts of the ISPS code also cover cyber security aspects:

> "ISPS Code Part A
>
> 15.5 The port facility security assessment shall include, at least, the following elements:
>
> .1 identification and evaluation of important assets and infrastructure it is important to protect;
>
> .2 identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures;
>
> .3 identification, selection and prioritisation of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability; and
>
> .4 identification of weaknesses, including human factors, in the infrastructure, policies and procedures.
>
> ISPS Code Part A
>
> 16.3.3 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface; "

The Regulation (EC) No 725/2004 applies within the European Union and it makes also some of the Part B mandatory. This is further clarified in chapter 3.1.2.

The ISPS Code has not been updated since it came into force 2004 but it can still be a useful regulatory tool also for cyber security threats. One must keep in mind the fact that the ISPS Code was created for physical security and not specifically for cyber security.

This means that in will not cover all aspects but as mentioned, can provide some directions on what to take into account.

The ISM Code in its current form was adopted in 1993 by resolution A.741(18). It was made mandatory on 1 July 1998, by a new chapter (chapter IX) in the SOLAS Convention. The purpose of the ISM Code is to provide an international framework for the safe management and operation of ships and also for pollution prevention. The ISM Code applies to ships and shipping companies and it has been amended several times over the years.

Cyber security obviously can be seen as part of risk management. The IMO has agreed that cyber risk management should be part of existing risk management system. Therefore, IMO Resolution MSC.428 (98) encourages shipping companies and managers to assess cyber risk and implement relevant measures covering all functions of their safety management system:

> "NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,
>
> 1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;"

According to that resolution, cyber risk management should be covered in the safety management systems “no later than the first annual verification of the company's Document of Compliance after 1 January 2021”.

The IMO has also released Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) in July 2017. None of these resolutions provide a very precise framework for how cyber security issues should be resolved. Both of them leave much of the interpretation to the shipping companies. There is still a lot of uncertainty on the field about how these requirements should be handled.

Two of IMO’s committees (Facilitation and Maritime Safety) introduced a resolution in 2017 (IMO, july 2017, 1). The committees stated that they have:

> “considered the urgent need to raise awareness on cyber risk threats and vulnerabilities”

The STCW, International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, was adopted on 7 July 1978 and entered into force on 28 April 1984. The main purpose of this Convention is to promote safety of life and property at sea and the protection of the marine environment by regulating the standards of training, crew certification and watchkeeping. Some of the training requirements for all navigational officers, navigation at the operational level (STCW A-II/1), we recognized to be related to the ability to interpret information available, such as "obtaining and maintaining situational awareness" (IMO, 2011, 101). The training requirements related to technical equipment on-board, ARPA (Automatic Radar Plotting Aid) and ECDIS (Electronic Chart Display and Information System), state that the deck officer shall be able to understand the information these systems provide (IMO, 2011, 102-103). For qualification as Chief Mate and Master, navigation at the management level (STCW A-II/2), there is a more specific requirement related to navigation systems (IMO, 2011, 114):

> "An appreciation of system errors and thorough understanding of the operational aspects of navigational systems"

One could question argue the logic here, since qualification as officer in charge of a navigational watch means that the person may be the person in charge and partly alone on the bridge. How to interpret information and to be alert in case of possible malfunctions, wrong data or even failures, should be introduced from the beginning of the career and therefore set as mandatory in the international regulatory instrument.

However, as we study the training requirements at the management level further, we find that the knowledge of updating system software as well as managing back-up files related to ECDIS are included in that table (IMO, 2011, 114). There is a difference between defined competences for the different levels and therefor an assumption of their tasks on-board? Of course, we must keep in mind that these are *minimum* level of training requirements but due to the globality of the maritime industry and cultural differences, there might be parties to the STCW Convention which stick to the minimum and that would result in the following:

a) Deck officers have the responsibility to understand radar and ECDIS-information when making decisions

b) Deck officers may have only general knowledge about the systems and are not introduced to system errors nor the functions of updating and keeping back-up as appropriate

3.1.2 EU legislation

According to Ringbom (2008), the majority of EU maritime safety rules are based on international rules. The EU is more of an implementing body than a regulatory body (Ringbom, 2008, 503). However, the EU has additional unique legal instruments, for example Directive 2005/65/EC on enhancing port security. This directive regulates port security and it complements the EU regulation 725/2004.

Fundamental legal instruments within the EU legal framework are regulations and directives. A "regulation" is a binding legislative act. It must be applied in its entirety across the EU and is valid as such, no need to rewrite it in national legislation. A "directive" is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to their own laws or devise existing legislation to cover the requirements in a directive.

The European General Data Protection Regulations (GDPR) sets rules for the handling of personal data and entered into force on May 25th, 2018. It is applicable to organizations also outside the geographical area of the Union, if the data subject is an EU citizen. In short it sets mandatory standards for the protection of personal data, which does not mean that individuals can prevent their data to be used. The regulation states that appropriate use must be allowed in order to guarantee smooth flow of data when needed to perform functions within the society, both public and private sector. Not all handling of personal data requires direct approval by the subject. By setting same level of standards within the Union, other authorities and organizations can rely on same requirements and protections in other countries. This enhances the flow of personal data when needed and also sets protection requirements. Personal data shall only be used for relevant processes by designated persons, it must be stored and deleted in accordance with the needs. Companies must show that their handling of data is compliant with the regulations. Regarding sensitive data, such as information related to health, special secrecy shall be applied. (EU, 2016, 2, 35-36, 38-39)

As mentioned in chapter 3.1.1 we revert to the Regulation 725/2004. The ISPS code has been implemented within the EU by Regulation (EC) No 725/2004. This Regulation makes also some of the Part B mandatory (Regulation (EC) No 725/2004, Article 3 paragraph 5):

> "5. Member States shall conform to the following paragraphs
>
> of Part B of the ISPS Code as if they were mandatory:
>
> - 1.12 (revision of ship security plans),
>
> - 1.16 (port facility security assessment),
>
> - 4.1 (protection of the confidentiality of security plans and assessments),
>
> - 4.4 (recognised security organisations),
>
> - 4.5 (minimum competencies of recognised security organisations),
>
> - 4.8 (setting the security level),
>
> - 4.14, 4.15, 4.16 (contact points and information on port facility security plans),
>
> - 4.18 (identification documents),
>
> - 4.24 (ships' application of the security measures recommended by the State in whose territorial waters they are sailing),
>
> - 4.28 (manning level),
>
> - 4.41 (communication of information when entry into port is denied or the ship is expelled from port),
>
> - 4.45 (ships from a State which is not party to the Convention),
>
> - 6.1 (company's obligation to provide the master with information on the ship's operators),
>
> - 8.3 to 8.10 (minimum standards for the ship security assessment),
>
> - 9.2 (minimum standards for the ship security plan),
>
> - 9.4 (independence of recognised security organisations),
>
> - 13.6 and 13.7 (frequency of security drills and exercises for ships' crews and for company and ship security officers),
>
> - 15.3 to 15.4 (minimum standards for the port facility security assessment),
>
> - 16.3 and 16.8 (minimum standards for the port facility security plan),
>
> - 18.5 and 18.6 (frequency of security drills and exercises in port facilities and for port facility security officers)."

Some of the above mentioned mandatory requirements are clearly related to cyber security. In particular the paragraphs 15.3.5 (radio and telecommunication systems, computer systems and networks) and 16.8.7 (procedures to assess the continuing effectiveness of security measures, procedures and equipment, including identification of, and response to, equipment failure or malfunction).

Finally one relevant directive should be mentioned, namely Directive (EC) 2005/65 of the European Parliament and of the Council of 26 October 2005 on enhancing port security. This Directive complements the Regulation 725/2004 and it is implemented by our national legislation.

3.1.3 National legislation

National law related to international voyages is covered under the same principles mentioned in the previous chapters. Finland has a wide range of national legal instruments concerning both domestic and international shipping. The main technical act is “Act on the Technical Safety and Safe Operation of Ships”.

Manning, safety management and crew certification are regulated by three main instruments: Act on Transport Services (320/2017), Act on Ships' Crews and the Safety Management of Ships (1687/2009) and Government Decree on the Manning of Ships and Certification of Seafarers (508/2018).

The most important national act in the context of maritime security is Ship and Port Facility Security Act (485/2004). Among other things the Port Security Directive 2005/65/EC is implemented with this national act. The maritime security tasks of competent authorities are also covered here.

It is not relevant to go deeper into the whole wide range of Finnish maritime legislation. It can be highlighted as an important conclusion that the international legal framework has been implemented through national regulations and related to maritime cyber security, there are no specific requirements at national level.

3.2 Previous research

Technical development within the maritime sector has been presented by Fitton et al. (2015) in a report published by Lancaster University on cooperation with the UK

Government. The material is based on a workshop. It covers both technology and human element -aspects and results in various recommendations for the maritime industry. We refer to this report in our study, which is much more limited and detailed; the team of experts who conducted the workshop and its results have made general observations for maritime security, while we have the limited scope of Finnish shipping companies and ports. Three elements were defined when forming the framework for cyber security – information, technology and people. In our study we will focus on the "people" part but we also must understand the connection between people as *users* of "technology" and "information" (Fitton et al., 2015, 2). Where does the malfunction in a process become a human error and when it is clearly a technical issue?

Thesis: WMU, David Miranda Silgado, "Cyber-attacks: a digital threat reality affecting the maritime industry", 2018. This study presents cyber-attacks to the maritime industry from the past seven years and via them the author analyses risks related to cyber security and presents recommendations of actions to minimize risks. It also included a questionnaire to administrations and shipping companies in order to get a view on cyber security awareness in the maritime sector. This thesis includes more information about possible consequences, such as environmental pollution, which we have decided to leave out.

Pajunen (2017) studied both human factor and technical aspects in his thesis with the title "Overview of Maritime Cyber security" (Pajunen, 2017). There were two main goals in his study:

1. To find out what kinds of networks are used on-board vessels and their level of security
2. To find out the level of information technology skills and security awareness among Finnish officers

These objectives differ from ours. Pajunen's second part of it is related to knowledge, such as our study, but limited to Finnish officers. We have looked into the situation in general seen from the company management's point of view, since that is where processes are agreed upon and prioritizing, planning and decisions made. The users on-board implement the outlines. The security and safety of the ships lie to a large extent in the officers' hands, but not completely. The research was done with a questionnaire, basically only yes/no-answers. Pajunen admits that the number of answers (17 deck and engine officers) is rather low, which also supported our choice of collecting data.

Pajunen suggests that a cyber-security related training course should be introduced for the officers and he has listed some fields to be covered. Another recommendation from that study is the introduction of an IT-officer on-board. As described it may be too heavy for the smallest shipping companies and ships, since the IT-officer would not have any navigational watch keeping duties.

Pajunen's thoughts about the IMO's guidelines on cyber security are not very positive. He feels they are too vague and do not provide any real advise to shipping companies (Pajunen, 2017, 9). We, on the other hand, see the link between the ISM Code and IMO Resolution MSC.428(98); they are built up to give enough freedom to the operators also bearing in mind the size of the company, its vessels, vessel types, trading area and last but definitely not least: its level of technology and connectivity. The IMO cannot take full responsibility for protecting the maritime industry. The IMO consists of member states covering most of the world and with its present legally binding instruments, there is a heavy burden on shipping companies to cover. Introducing a new, massive set of rules covering all kinds of ships and levels of technology would be an impossible task and meanwhile nothing happens as the whole industry waits for a detailed set of rules for them. This is something the shipping companies and ports must do themselves in the most suitable way for them. Quoting Ulsch (2014, xvi):

> " "security" and "technology" are two words that every board director must embrace because these two words result in two other words that the board understands all too well: "risk impact" "

Furthermore, Pajunen is stating in his conclusions that this subject should be studied further and that there is room for improvement regarding cyber security awareness (Pajunen, 2017, 42-44).

When looking at the human element in relation to a rapidly developing field, such as information technology, we wanted to look at older material, too. A study from 1995 conducted by the United States Coast Guard had its primary purpose in proposing US' comments to the Performance Standards for ECDIS, which had been introduced by the IMO. In order to do so, the USCG conducted route monitoring in accordance with the standards. The aim was to find out the benefits of the use of ECDIS; would it reduce the workload of the navigator and would it contribute to safe navigation. The study also included integration of electronic chart and vessel positioning system. It is fascinating to read the previous studies presented in the USCG document; the authors state that during the last ten years (1985-1995) USCG has actively been researching the human element in relation to "potential effects of new, developing technologies on navigational performance". From the navigator's point of view, one clear advantage occurred when integrating radar and ECDIS; they could get al.l the information from only one display and the addition of a navigational chart to the radar made the identification of targets easier (United States Coast Guard, 1995, 1-1, 1-2, 1-5,. 7-4). Some concerns were similar to those we struggle with today; users might want to see different setups on their ECDIS/radar display, the users must know what data is available to them and they must understand the data they look at (United States Coast Guard, 1995, 7-4). Other than that, the current challenge of cyber security was not covered in this study.

This study was basically not relevant for us, because the study would not dig into the world of risks from new technology, nor focus n possible technical errors whish the navigator should react to. Interesting reading, though! Same insecurities with new systems then as it is still today; both in the role of the user and also the technology.

Svilicic et al. (2019b) have conducted a cyber risk assessment by interviewing the crew of a training ship. The focus was on the ECDIS on-board.

There have been studies on how personalities have an impact on cyber security behaviour. For instance, calm and rational people tend to detect phishing e-mails better than those with personality qualities such as being extravert and anxious. Some of us are more considerate and cautious than others. Hadlington (2017) found some inconsistencies in previous studies related to human traits and wanted to conduct a study of his own. The aim was to find out how impulsivity, Internet addiction and attitudes of employees affect risky behaviour. Our study does not dig into human personalities, but it is an interesting point-of-view. Maybe something for organizations to understand and take into account, that different people might need different kind of guidance to ensure cyber-secure behaviour? Especially those in critical tasks and with access to safety-critical equipment and systems. Depending on the field of business, focus on recruiting the right people and also covering this aspect can be of various importance. Our scope is the maritime industry, where organizations need experts in those areas. During the recruitment process the decision-makers cannot override appropriate educational background, experience and other requested qualities simply because the first choice might be a little more anxious then the next in-line and more probably be clicking on malicious links in e-mails and thus might cause a higher risk to the company. A little bit farfetched from the reality, as we see it at the moment! Problems like this should be covered by proper familiarization, internal guidelines and clear processes.

Another study also conducted by Hadlington (2018) looked into the links between the size of a company, its employees age and attitudes and how these factors have an impact on cyber security behaviour. Hadlington emphasizes the risk from inside a company, especially the unintentionally caused breeches, which might be overlooked (Hadlington, 2018, 2). Despite the importance of identifying crucial functions within a company, among workers and their behavior, our study is conducted at a general level and we have not dug into attitudes at a personal level neither looked for correlations between certain personal factors and cyber security awareness. We have made a more general research.

Kusi (2015) has conducted his bachelor's thesis as a case study on Takorandi port of Ghana. Both geographically and culturally rather different than the Finnish ports, which are the scope for our study. The objective in that study was to find out threats and vulnerabilities, whereas our aim is to define the level of understanding and preparedness from the human element -perspective; not to identify specific ship- nor port-specific risks. Kusi has identified risks related to port activities.

Ahokas and Kiiski (2017) have conducted a general study on cyber security in ports. It describes different types of ports and possible risks related to them. We found it useful as a part of our research and base for presenting risks related to ports. The main threats listed in that study were intentional, such as hacktivism and cyberterrorism. In our study we will also include unintentional events, careless or negligent behaviour leading to cyber security -related incidents.

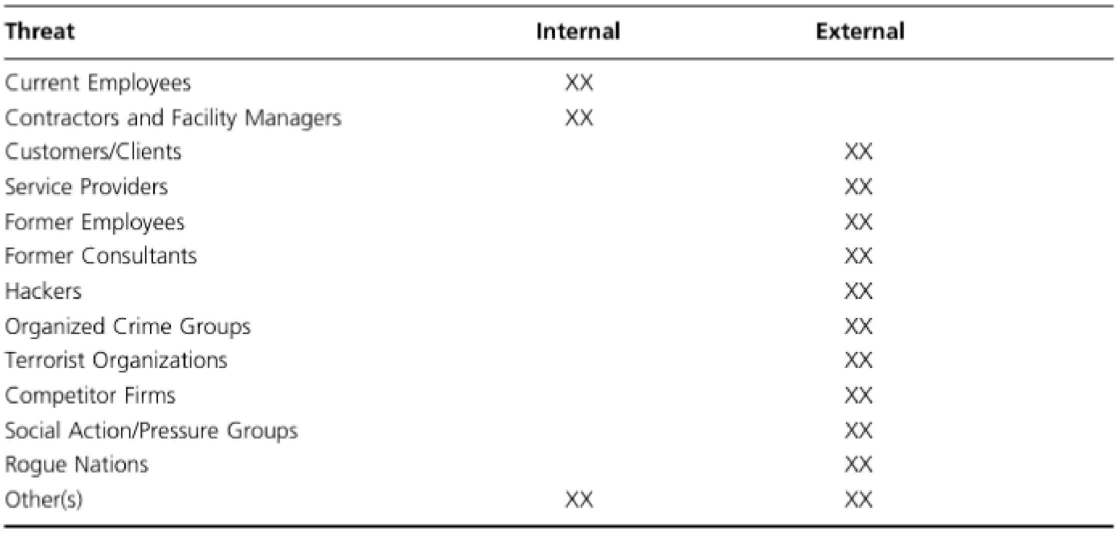
Understanding human behaviour when taking actions and making decisions related to cyber security is important. There is evidence of some users to cause a higher risk than others. Gratian et al. (2018) have themselves conducted such studies and they refer to other research in the field. This kind of approach is not of relevance to us in our work – even though highly interesting! Should there be a study on different professions, marine professionals included, and the correlation with cyber security incidents, we would be very interested!

4 Cyber security and the human element

Before being able to identify the risks which shipping companies and ports may face, we must recognized the roles involved in the processes related to cyber security.

A common view is that problems related to the cyber world are considered to be technical, not related to operation (Ulsch, 2014, 3). This means that operators may overlook the human element or not provide resources to develop competence in this field but focusing on solving pure technical risks.

McNicholas has identified and divided the groups of people which may pose a threat in this picture:



Threat	Internal	External
Current Employees	XX	
Contractors and Facility Managers	XX	
Customers/Clients		XX
Service Providers		XX
Former Employees		XX
Former Consultants		XX
Hackers		XX
Organized Crime Groups		XX
Terrorist Organizations		XX
Competitor Firms		XX
Social Action/Pressure Groups		XX
Rogue Nations		XX
Other(s)	XX	XX

Figure 7. Persons in different roles can be a threat to cyber security (McNicholas, 2007, 375)

This is a fundamental base to be able to identify where the human related risks are. We feel it can help our target group when creating their cyber security management system. These roles may also form threats to security in general, not only cyber security.

It is self-evident that current employees are a risk due to the accessibility; they have permits to enter different locations within an office or a ship and also access to different kind of data that can be obtained. This accessibility can be used for different goals; as vengeance for some unfair treatment or in order to achieve financial benefits. (McNicholas, 2007, 375)

On the other hand, permanent employees might be more trustworthy than short-term substitutes, who may not experience loyalty towards the company. Recruitment is very important also from the security aspect and in some companies to some positions (eg. security guards in a passenger vessel) might need background-checks.

Hackers, organized crime groups and terrorists are a group of people unknown to the company. Since they are unknown, they are most difficult to identify or detect. They represent a risk and the company and its employees must keep in mind that someone somewhere might deliberately want to cause harm to them. Some are random hits while others are aimed at a particular target. The random hits may be easier to control, as attackers choose the systems and networks which they are able to get access to; e.g. those that are lacking appropriate protection measures. On the other hand, targeted attacks have an aim defined by the attackers, often a financial benefit. In these cases maybe not every small Finnish cargo shipping company is of value, while random hits can become reality also for the “not-so-interesting” targets with no identified value such as valuable cargo or many passengers.

The different roles involved in a company’s business and with different kind of access to information systems, databases and networks, need to be identified by the company in order to detect the human element as a risk. We will address this in our field study.

Another listing of different roles behind intentional attacks has been made by the National Cyber Security Centre (NCSC). These roles were adapted by BIMCO et al. (2017, 6), which is a maritime industry -driven set of guidelines. This means that the roles are relevant also for this study. Tam and Jones (2019b, 6) have listed the different roles and here we have concluded them and their motives based on these three sources:

- **Hacktivists** with the same agenda as activists: causing damage due to political or ideological reasons. The target would then be organizations involved in such activities and processes or with strategic goals that are against the hacktivists’ ideology

- **Competitors** who either want to obtain information about current agreements or manifests for their own use or simply to cause financial and/or reputational damage such as data breach and thus gain own advantage

- **Criminals** usually want economic benefits. The means to achieve that can vary; selling data as such or requiring ransom for not revealing it or using blackmail. In the maritime industry information can be used to enhance physical crimes, such as information about vessels or their valuable cargo

- **Opportunists** work for someone else. They are involved because of the challenge; is it possible to get in and what information can we retrieve? The information or service if causing damage is paid for so the benefit is financial

- **Terrorists** are likely the only group who seek to cause damage and deaths to humans. The other may also cause it directly or indirectly, but most likely that was not the intention. Terrorists want to cause damage and they might use data retrieved for own use or for getting information about the organization to plan further

- **Employees** as well as contractors or other groups of people with approved access to facilities, systems and networks may cause an attack. The goal is similar to that of hacktivists; causing damage or public attention. The attack can be caused intentionally if they feel mistreated or for other reasons want to get back. In addition, an attacker can use an employee for different purposes, e.g. directly by blackmailing to get the legitimate person to perform required actions or by the use of social engineering, as presented in section 6.3

A relatively small group behind intentional cyber-attacks are **elitists**. As the opportunists, elitists are in for the challenge and satisfaction of breaking the cyber protection. Their goal is not to cause damage, but it might be an unintentional result.

We move further from the divisions on people in segments and see that one of the first, maybe most obvious roles for the human element in the cyber world is as the employee as a *user*. A user has tasks which shall be done. When the tasks require manual logging in with a self-defined password and the user has the responsibility to keep anti-virus-protections up-to-date him-/herself, we discover a security risk. Studies have shown that a majority of users do not identify lacks in their own computers such as un-updated anti-virus software (Voeller, 2014, 42-43). In some cases there might be outdated software in use, which no longer is supported by its creator (Fitton et al. 2015, 8). Regarding users and their knowledge: the user will need different kind of knowledge depending of the company, tasks, type of hardware and software and data they handle. Phishing-mails, interesting links sent by someone you know and attachments containing viruses are definitely a threat where the user plays a major role in the outcome (Voeller, 2014, 44-45). Of all the roles listed here, the internal users are probably the easiest to define and to control by the organization. To conclude: is everyone appropriately familiarized, instructed and trained?

Next we have looked at ship- and port-specific roles. The operational processes and connectivity are different on a ship and in a port. Therefore we have looked at the different roles from that particular perspective. In chapters 7 and 8 we have listed the recognized risks for these organizations.

4.1 Human roles within shipping companies

In the previous section we looked at the different aspects of the human element related to maritime cyber security in general. In this and next sub-section 4.2 we have more clearly defined the roles within a shipping company and a port and left out external roles, because they are out of the organization's own control and their actions cannot be influenced. Roles in the office depend on the type of operation – cargo/passenger – and type of structure such as chartering contracts.

From ashore the most relevant tasks:

- Overall management (Designated Person Ashore), responsibility for the ISM-system within the company covering both office and shipboard processes and documentation

- Crewing management (including recruitment, employment, coordinating crewing issues on-board). All of these processes include personal data storage and e-mail correspondence between ship and shore and may include IT-systems which are linked to the ones on-board

- Business contracts including economic aspects: outsourced or in-house, handling of business-sensitive data and control thereof

- Customer-related functions for passenger companies (contact with passengers, marketing, bookings)

- Subcontractors, suppliers, technical service (including information technology and operational technology)

The land-based functions and thus roles included have a major impact on how risks are managed on-board.

Shipboard personnel implement the requirements and instructions from international and national authorities as well as company-specific. Technical equipment and service thereof are ordered, deliveries received and installed, service personnel advised and authorized. Employment contracts can be agreed upon and salaries paid. All of these need communication and more so electronically and via internet connection. Recreational usage of internet as well as professional occurs on-board.

The navigator on-board a ship has a huge amount of data to control and use as a base for decision-making. The technological development has made the data easily accessible and interpreted. However, as the systems become more and more complicated, connected and the number of displays on the bridge increases, there are some challenges for the navigator too, and the IMO (2007) has acknowledged that. When introducing Integrated Navigation Systems on-board and standards related thereto, the IMO has also presented some requirements to the system. If an integrated navigation system is in use, it should be easy to use by "a trained user". Furthermore, the system should "minimize the risk of human error" and it should not distract the navigator from the core task – navigating. When the INS requires manual input, it should double-check with the user and ask for confirmation.

Safety management systems shall be implemented on-board. This system shall cover, among other things (IMO, 2014, 15):

> "Instructions and procedures to ensure safe operation of ships"
>
> "Procedures to prepare for and respond to emergency situations"

These are rather large entities and furthermore there shall be descriptions on how the company will reach those goals. The processes are related to the human element.

BYOD (Bring Your Own Device) causes a risk when crew (or passengers) can connect their own devices to the shipboard network. Being able to browse on the internet and even more importantly, keeping contact with loved ones via social media and e-mail, is an important part for a seafarer's wellbeing today. The company should also acknowledge this and be aware of the connections; what can be the consequences for the shipboard network and systems when during private use on a personal device an employee clicks on the wrong kind of link or opens a harmful attachment. (BIMCO et al., 2017, 17)

4.2 Port-specific roles

The authors of this document are very familiar with the maritime industry in Finland. We understand that cyber-attacks or malfunctions in port systems may cause more damage than that of shipping companies, since the ships are not connected 24/7 but the ports are. Ports can be complex facilities even if the core organization consists of a limited number of employees. Depending on the port and cargo types, there might be truck drivers, stevedores, seafarers from a ship in port, passengers, authorities, agents, shipping company representatives, seaman's service bureau representatives, delivery and service providers or other sub-contractors coming and going in the secured port area. The work is hectic and supply chains must be smooth. Are all security- and identity-checks appropriate without having an impact on the daily work?

Ports have an organization of their own, consisting of internal users. These tasks depend on how the work is administered by the port itself and how much is left to subcontractors. Processes involving humans are listed by Ahokas and Kiiski (2017, 21):

- Administrative functions are related to paperwork and control, such as control of dangerous cargo, immigration, customs

- Operational functions can be mooring, pilotage and processes related to cargo operations and storage

5 Information Technology, equipment and connections

Most of the crucial equipment and systems are located on the ship's bridge and are related to navigation, including control over propulsion systems and communication. Equally important are engine room systems which are critical to vessel operation. There might also be computers in deck offices, Master's cabin/office and Chief Engineer's cabin/office. On larger ships, also other capacities may have their own devices.

We recognize that ships of different size, type, trading area, nationality and age have a different level and amount of technical equipment and networks. Here we will list the minimum and recognize that is not all-inclusive. Some of the technology is mandatory, such as AIS and ECDIS. Because of the vast amount of varieties within shipping companies and ships, we decided not to focus on the specific systems on-board or ashore (company offices and ports). We will only mention them and not describe them. The purpose of our study is to focus on the awareness among Finnish shipping companies and ports and to increase awareness. For these purposes a thorough report on the different equipment, connections, networks and systems is not appropriate. However, since ECDIS is a very central and can be largely connected to other systems on the bridge and also connected, we will make some research into the cyber risks related to ECDIS.

The IMO has set some standards for the Integrated Navigational System INS (IMO, 2007). These standards are recommendations but present relevant equipment, so therefor we use it as a reference. The aim with INS is to provide the navigator with as much easily-read data as possible as a support for decision-making or as backup. IMO presents the following systems and their tasks (IMO, 2007, 5):

- Radar system
  - collision avoidance
- ECDIS
  - route planning
  - route monitoring
- Heading control system (HCS)
  - navigation control data or
  - navigation status and data display
- Track control system (TCS)
  - Navigation control data and track control
- Presentation of AIS data
  - Collision avoidance
  - Navigation control data

- Echo sounding system
    - Route monitoring
- EPFS
    - Navigation control data or
    - Navigation status and data display
- SDME
    - Navigation control data or
    - Navigation status and data display

ECDIS is nowadays mandatory on all ships. It is also accepted as an adequate alternative to carrying paper charts on-board (IMO, 2009, 3) An analysis on ECDIS vulnerability resulted in six cyber threats of different severity and probability. The weakest points are the operating system, its relevant setup and updates as required. When ECDIS is connected to the internet, there is also the risk of being attacked by a hacker (Svilicic, 2019a, 234-235).

There are other systems and equipment on-board which are not related to navigating but can cause damage if controlled by the wrong hands or due to malfunction. Here some listed by Tam & Jones (2019b, 19):

- inert gas system (used in oil tankers to prevent explosions by filling up the free space in cargo holds with low-level oxygen)
- protection and maintenance systems such as cooling, heat and ballast water
- engine control rooms

User-related standards are presented earlier in this document. IMO also set requirements on technical back-up and redundancy. We will not dig into them here but they should be used as advice when designing an INS (IMO, 2007).

Additionally to the ones included in INS, bridge equipment and systems is also listed in the ICS Bridge Procedures Guide (ICS, 2016, 60-62, 65-66):

- Steering gear and autopilot

- Compass systems

- Speed and distance log

- Global Positioning System

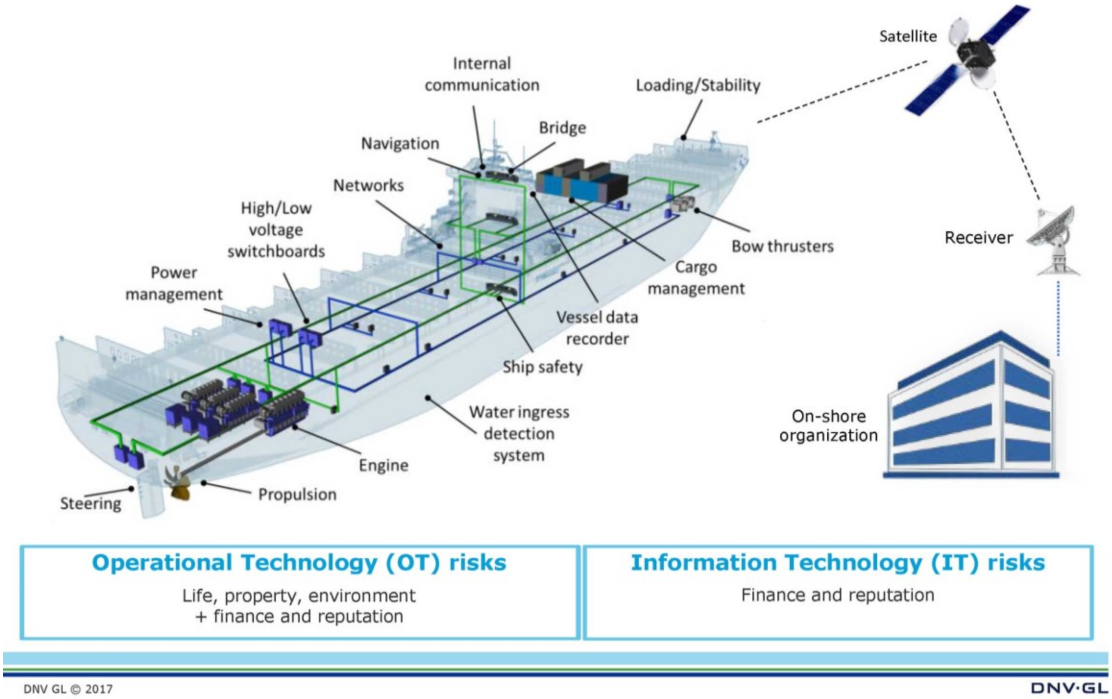


Figure 8. A descriptive illustration on ship's connectivity (Ording, 2017)

The greatest decisive factor the vulnerability of systems on-board is whether they need to be connected or not. The level of networks and connections may increase as automation and remote-control emerges. Especially if a ship is in irregular trade where the voyages are determined by a chartering department ashore, it is evident that a connection for this information is required. The more data that can be exchanged via mutual systems, the easier for the employees. On the other hand, a non-connected system will then probably need to be updated by a physical device, removable media and that is a risk. Integration within a ship makes operations on-board easier when information is transferred between systems, such as propulsion power and steering information, but on the other hand make the IT-systems vulnerable; an interruption in one part affects others. (BIMCO et al., 2017, 10).

The ICT-systems in ports are to some extent the same as for shipping companies and ships, such as e-mails and use of removable media to company equipment. Authentication of physical as well as network access are mutual factors. Some ports have automated processes which can be hacked.

As is the situation for shipping companies and ships, also ports represent a wide variety of categories and sizes. Three basic types of activities have been identified by Drougkas et al. (2019, p. 15): activities related to maritime cargo, transport of passengers and fishing. In our case the latest mentioned is not of relevance. The infrastructure, including technology, required to carry out these processes is naturally different.

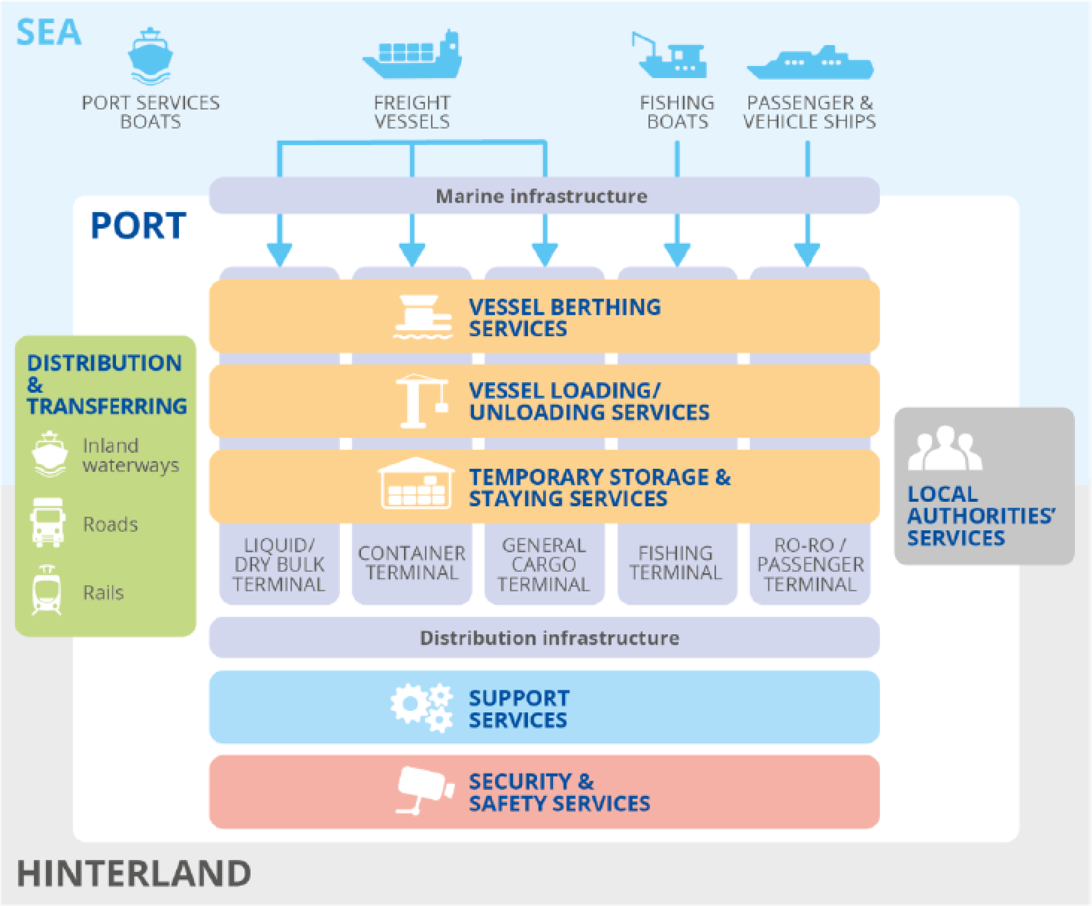

SEA
PORT SERVICES BOATS
FREIGHT VESSELS
FISHING BOATS
PASSENGER & VEHICLE SHIPS
Marine infrastructure
PORT
VESSEL BERTHING SERVICES
VESSEL LOADING/ UNLOADING SERVICES
TEMPORARY STORAGE & STAYING SERVICES
DISTRIBUTION & TRANSFERRING
Inland waterways
Roads
Rails
LIQUID/ DRY BULK TERMINAL
CONTAINER TERMINAL
GENERAL CARGO TERMINAL
FISHING TERMINAL
RO-RO / PASSENGER TERMINAL
LOCAL AUTHORITIES' SERVICES
Distribution infrastructure
SUPPORT SERVICES
SECURITY & SAFETY SERVICES
HINTERLAND

Figure 9. Activities related to operations in port (Drougkas et al., 2019, p. 16)

In order to carry out these tasks smoothly, information must be transferred fluently and uninterrupted. The level of digitalized and automated processes is different in different ports and as for ships, the appropriate level of cyber security measures should be implemented.

ENISA in its report (Drougkas et al., 2019, p. 19) has identified data transmissions related to port operations, which include information required of the shipping companies by international regulations, authorization of persons entering the port and for instance involved in cargo operations, operational data for vessel support activities (coordinating cargo operations and need for bunker), financial data such as payments and navigational data (keeping track of vessel traffic via AIS).

6 Identified cyber risks

The risks around cyber security are different depending on the industry and size of the company. Which interest does it have to possible deliberate attackers? Impacts on large and widely automated manufacturing or distributive processes are assumably greater than in smaller, more manually arranged tasks. The damage on a well-known company's reputation as a result of a data breach can have serious consequences while a smaller one gets away without publicity. On the other hand, smaller companies do not have their own IT-departments which would be clearly responsible for the cyber security and make sure processes and awareness is at an appropriate level (Ulsch, 2014, 5-6). In the end, keeping the company's information technology and data protected will be cheaper than cleaning up after a data breach or after having lost faith in customers or other stakeholders. Direct financial consequences are loss of money or blackmail and system cleaning and upgrades will be required. Production or deliveries may be on hold during the clearing after an attack which naturally has an impact on the business and its revenue. Furthermore, the total effect of a cyber-attack may take a long time, an undefined amount of time, to sort out. Likewise the total financial loss. (Ulsch, 2014, 72-74, 76)

Third parties include a risk in itself. They are not in the core business, may not be as aware and protected and thus form a possibility for cyber-attackers to use. A long history of cooperation between organizations might give a false indication that the level of mutual trust and liability is high. Management and employees have changed during the years, the third party's economic stability may not be as it was years ago. It is not the same company as it was when the previous, closely involved managers once signed the agreement to become partners in business. (Ulsch, 2014, 145-146, 151) The maritime industry in Finland is small and this risk can be reality, when there are many small businesses and people involved in them are familiar with each other.

We have now studied previous research and the role of the human as well as technological equipment. Based on that, in this section we have listed the most important cyber risks related to the human element. The list is appropriate for both ships and ports but is not all-inclusive.

6.1 Denial of Service (DoS) -attack

Increased connectivity mean increased attacks caused by denial of service, where a device or network is overloaded with information and the correct signal cannot reach its target or the real user cannot access the information needed. An example is rudder angle information which does not reach the indicator on the bridge. (Tam & Jones, 2019a, BIMCO, 2017, 8)

6.2 Authorization

Authorization and limitation of access is an effective way to control internal damage. Voeller (2014, 10-13) discusses policies for access to sensitive or no-to-sensitive information within the company for instance via ACLs (Access Control Lists). We think that this will vary depending on the size of the company; if only a few users, access is easier to limit and keep up-to-date whereas a multi-national company with many users might be more difficult to control and among more users the risk for intentional malpractice is more evident. In a smaller company, responsibilities are shared between fewer people, which means that restrictions in getting access to information is less complicated; only one HR Manager and one HR Assistant both need access to all HR-related issues. A large HR department with a separate Payroll Manager and a Manager in Occupational Health cannot have access to the same data. McNicholas (2007, 370) mentions restrictions in access and level of rights to be defined in the system in order to minimize the responsibility of the workers.

Regarding access to company information, the outsourcing of information technology issues means that outsiders are granted access. The company should determine the level of confidentiality and define how the information should be protected. (McNicholas, 2007, 368)

In lieu of leaks in the authentication or accessibility processes data may also be the target for deliberate actions, such as hackers. A competitor can use information to increase their own performance or cause harm to the company (and therefor benefit to itself) by reporting about personal data leak. (McNicholas, 2007, 376)

Ship Security Plans (SSP) should already cover the physical access on-board, so regarding the ships this part ought to be covered. (BIMCO et al., 2017, 5). Also ports need to have Port Security Plans according to ISPS regulations.

We conclude that wrong data in the wrong hands is one general cyber risk that can be divided into internal data breach (wrong people have access) and an external source deliberately obtaining company-sensitive information for their own purposes.

6.3 Social engineering

Social engineering (Hadnagy, 2014, 5-18) is a broad set of harmful acts, contacting a person directly. It involves nonverbal communication, which consists different parts of the body communicating; facial expressions, eyes and hand movement (emblems). It also includes *how* the communicator speaks (rhythm, speed, volume and pitch), from which an observant and skilful nonverbal communicator can draw conclusions. In short: happy, confident and positive faces and body language build up trust between the social engineer (with devious intentions) and the target (with desirable assets or information). If the social engineer is nervous, worried and even afraid and it is shown in the nonverbal communication, it will also cause insecurity in the target, who might become suspicious and suddenly is not such an easy target. The above description is mainly applicable to face-to-face contacts, but why not also in over-the-network contacts. The purpose of this description is to note that manipulation may be revealed on the basis of abnormal behaviour.

Unauthorised persons can be able to enter buildings by tailgating; following people who do have access. By joining a party of smokers outside an office building, it can be easy to enter together with them. Other similar possibilities for literally opening doors are when carrying something (you obviously need help to open the door) or wearing a fake badge. This is called tailgating. The badge is not supposed to work but when other employees sees your efforts, they of course want to help and let you in. In all these situations the skilful social engineer makes you feel comfortable and secure and does not give any reason for suspicion. (Hadnagy, 2014, 45)

These issues arise when someone with bad intentions persuades someone else to take actions which may not be in their own best interest – we can even call it manipulation. Social engineering is to a high extent a risk involving the human element. With a little research, appropriate clothing, name tags on the shirt, persuasive and confident communication and identifying oneself with the target group, it is possible to retain information or access without being an information technology engineer, but a social engineer. (Hadnagy, 2014, 43)

Social engineering is a common way to attack also via networks. The cyber-criminals can for example act as IT support personnel and try to manipulate access for themselves to the company's IT system. It is also the kind of attacks a company can protect itself from by raising awareness among its employees. (Salmon et al., 2017, 16)

We think that the risk of being a target of social engineering is bigger in larger companies, where not every employee and delivery are known to everyone. Instead it is a part of everyday work and routines to have people coming and going, calling, ordering, delivering and so on. The logistic chains must be smooth and not cause delays. This sets limits on how much time and energy the workers can spend on checking subcontractors' identities and verifying their access rights, either technical or physical.

Social engineering includes different sub-types, and can also be combined with other of the risks presented further in this chapter, such as placing a jamming device on a ship.

Transmission of data over a network within a company is on the other hand a requirement today but on the other hand makes the process vulnerable for attacks. Sniffing and spoofing are two kinds of deliberate actions from the outside to achieve own goals. A sniffer would obtain user identification data and then be able to access a company's sensitive information. Spoofing means using false identity or pretending to be in another role, someone tries to gain own benefits (such as pretending to be a seller). (McNicholas, 2007, 373)

The above mentioned incidents are examples of social engineering. The aim is to via e-mail get information or a click on a link. In this kind of communication the social engineer would use emotions, like fear or threat (Hadnagy, 2014, 39). Furthermore, when trying to receive information by telephone and making it look like the call comes from a different number than the one actually calling from, spoofing, is also a means of social engineering. Already that can create trust and when discussing over the phone, it is easier to lie because facial expressions cannot be seen. It is fascinating how many actually have fallen for this kind of fraud and how easily people give their credentials, run malicious programs (believing it is cleaning up a virus which has hit the company) and even gives VPN credentials over the phone. All is based on the first belief that the caller is known and even within the company, in fact trying to help you. (Hadnagy, 2014, 40-41)

Phishing e-mails are sent out to a numerous of recipients, not targeting one specific. The aim to catch one or several; get them to open an attachment or click on a link which will cause damage. Pretexting is a kind of phishing where information is being requested directly by a false identity such as another department in the same company. In these cases the hacker takes advantage of trust between the recipient and the disguised sender. A hacker can also obtain information by baiting; offering something in exchange for information; by logging in with personal credentials the target would get a gift card. (Salmon et al., 2017, 125)

Spear-phishing is a sub-type of phishing, where the attack is aimed at an individual and it includes quite some research to obtain required information. A typical example is sending out e-mail in the name of the CEO requesting for sensitive data which then the recipients does not detect but reveals the information requested. (Salmon et al., 2017, 16)

Whaling is a phishing attack aimed at a high-profile target. (McDonough, 2019, 37)

6.4 Data breach

When sensitive information is leaked or someone unauthorized gains access, we talk about a breach. It can be the result of a mistake or an attack (McDonough, 2019, 8).

Apart from the individual mistakes, the company's own workers are not directly responsible for data breaches; provided that firewalls and other protective measures have been taken as appropriate and are updated. However, the users of company IT-systems can make an impact on to which extent damage is caused by realizing something is wrong depending on the level of knowledge of the user and on what kind of data breach has occurred. A data breach can (BIMCO et al., 2017, 9):

- cause changes to information on critical systems on-board, such as navigational equipment
- provide access to sensitive data related to persons or cargo

- give attackers control over a system, such as machinery management

It is evident that these kinds of attacks can cause comprehensive problems and damages for a company and its assets. Since the users by being aware and observant can make a difference in the outcome, training is of utmost importance (BIMCO et al., 2017, 9).

6.5 Personal data breach

We decide to add the handling of personal data as a separate risk, since personal data is handled by shipping companies due to IMO regulations. Recruitment processes require personal data. Documents of identification and competence as well as medical certificates shall be carried on-board. Port authorities require crew lists with different personal data. Information related to health is sensitive data and its handling is prohibited in accordance with GDPR. However, if such data is required for other legitimated process, handling with special care and limitations is allowed. Medical certificates are documents required by other legislations and shall therefor be included in personal data files on-board. (EU, 2016, 38-39)

6.6 Malware

In this study we decided to leave out technical risks. However, the human element is very closely involved in, if not the cause, then definitely the recovery of some technical failures, so we will include them to some extent.

Appropriate maintenance, back-up, updated anti-virus systems and firewalls are some issues which are in the hands of the company’s personnel. Malware means software used to cause deliberate harm to a company’s IT-system or in other ways achieve benefits for the planter of the malware. There are different kinds of viruses, new are being developed and they spread with different pace. Workers should be aware of how viruses can reach the company’s network – e.g. by opening suspicious e-mail attachments or links or installing free software, which has not been verified nor licensed. Via these channels, where people themselves actively allow entrance of the malware to the internal network and data, also spyware can be installed. (McNicholas, 2007, 377-378)

Malware can also be introduced by removable devices, such as USB-sticks. (BIMCO, et al. 2017, 1) Attackers could also provide a false “software update” on a removable media, which in fact is infected. Normal routine of a ship includes access to third parties;

subcontractors, port authorities and agents or pilots can request for access to shipboard systems or to “print documents” stored on removable, infected, media whether intentional or not. (BIMCO et al., 2017, 8-9, 14)

A sub-type of malware is called ransomware, where the attacker locks information the company needs and releases it once a ransom has been paid. E-mail attachments and links are one channel for malware to occur and this means that in practice it is the user who actually activates it (BIMCO et al., 2017, 7).

With adequate knowledge, sufficient back-up and agreed processes on how to handle e-mails within a company, the human element can either be the cause or the saviour regarding malware and viruses.

6.7 Jamming

Interfering in signals is called jamming. A jamming device, that can be delivered to the ship using skills of social engineering, is rather small and can be effective on ships, where signals from the ship can be weak and thus easily overridden. Jamming devices can be remotely controlled and used in different ways, such as interfering with communication from the ship. The main preventive measure lies in the processes, as a jamming device introduced on-board is difficult to detect. (Tam & Jones, 2019a, 9)

6.8 Malfunction and system anomalies

There might occur technical problems both in the ship’s engine room but also somewhere in the information technology systems on the bridge. These may be caused by non-deliberate actions; they just suffer from a technical failure and not cyber-attacks, but can also be caused by deliberate or negligent actions. However, we still want to include them in this study because of the involvement of the human element as an interpreter of the information received and as a decision-maker. For example if the ECDIS for some reason gives the wrong position and the officer on watch is being observant, nothing else happens. But the outcome can be very much different if there is no appropriate back-up, expertise and measures taken. So there is a technical failure but the human interaction, or lack of it, results in serious damage. The root cause of some technical failures might be in human negligence such as poor maintenance and updating of the systems. There are many examples of such accidents based on our own expertise and experience within the maritime sector.

All navigational officers should have received enough and adequate familiarization so they understand the importance of being observant and detecting possible errors in the software used on-board. The errors might be caused by a bug in the code or operation of the software and those cases are called software anomalies (ICS, 2016, 58-59). Many of us have probably experienced problems to occur after an update of a system and the reason can be in the human element – decoding some part of the software to make it better, causes an undesirable output somewhere else and the user realize that.

The human role can intervene when processing data received from different sources. On-board a ship, competence is important in order to evaluate information on the radar screen. The situation might even require the bridge management to use back-up processes instead of normal, more automatic ones. This is clearly a requirement for the humans on-board – are they qualified enough to understand errors and malfunctions and be able to operate despite malfunctions or cyber-attacks? (Fitton et al. 2015, 5)

7 Cyber risks: ships

Ships can be the targeted by a wide range of harmful acts, cyber-attack being one of the malevolent means in our modern world.

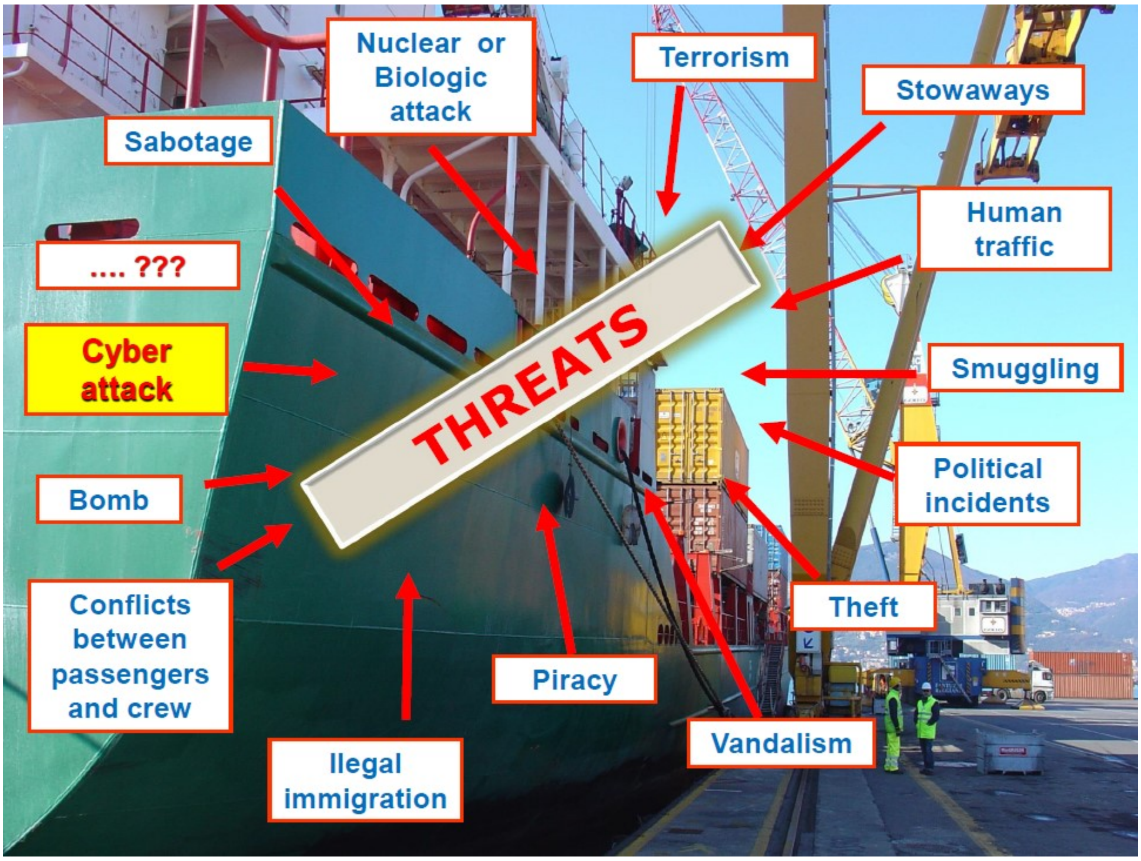


Figure 10. Presentation by EMSA, 6.3.2019 Maritime Cyber security Table Top Exercise, European Maritime Safety Agency's (EMSA)

Safety and security are familiar concepts within the maritime sector due to the highly regulated and globally controlled industry. However, cyber-security is due to its abstractive nature a fairly unrecognized threat. In general, the maritime sector has not been the first to implement digitalized and interconnected systems due to its nature. This makes it also vulnerable and attackers will discover it, since some attacks are not targeted at a particular company but try to get in where the firewall and other protective measures are at their weakest. As pointed out by Tam and Jones (2019b, 1-2):

> ”Normally, a system is considered functioning, or broken. However, with cyber-attacks, a non-functioning system may not be broken (e.g., a hacker can deny system access), and a functioning system may not be trustworthy (e.g., compromised systems can give false data despite seemingly functional).”

This is very descriptive. With bad connections on the ships, how can the seafarers identify a cyber security breach from “normal” slowly running systems on-board?

In this chapter we have graded the risks identified in accordance with likelihood and level of damage the particular risk can cause. During this study we have recognized the overall challenge between shipping companies or operators in the maritime industry – a small cargo shipping company may not be as connected, digitalized or attractive to cyber-attacks whereas the situation is very different for larger, globally operating companies with more valuable cargo or more economical assets to pursue. The latter kind would suffer more and may be more vulnerable to system failures (more damage can be done) and also more attractive to cyber criminals. Ironically, this more vulnerable and attractive, critical organisation with more resources available probably faces challenges with adequate training for its employees, due to the large amount of them (Jaf & al, 2018, 4987-4988).

On the other hand, one could speculate if some particular assumptions connected to a small and old-fashioned company in themselves are a risk. Those companies believe that "we only apply old technology so if one device collapses, nothing else happens and we can still keep up business as usual" or "our small business is not of interest to anyone". This issue of denial has also been raised by Ulsch (2014, 7). The company is even less prepared (ignorant) and possible attackers realize it.

The approach when classifying cyber security risks and their likelihood is rather different from that of classifying risks of an accident, which the maritime industry is very familiar with. It is not the likelihood which is crucial, but how easy it can be for an intruder to break in. An interesting aspect is the idea of an attacker using a system with easy access but no value, to reach other systems and more valuable information. (Tam & Jones, 2019b, 2, 7). This strengthens the fact that all connections between systems must be known as well as their protections. As stated earlier in this document: a chain is only as strong as its weakest link.

On-board a ship, the most important systems would be those affecting the ship's and crew's safety. AIS (Automatic Identification System) and ECDIS (Electronic Chart Display and Information System) are identified as critical systems with a high level of vulnerability. The AIS is vulnerable due to its connectivity. In some high risk piracy areas AIS may even be turned off to avoid being discovered. ECDIS' vulnerability is based on, besides its connectivity, the requirement for frequent updates via internet or USB, for example. Furthermore, it is nowadays approved to have another ECDIS as backup instead of paper charts, which was the requirement some years ago. The redundant ECDIS does, however, most likely have the same functionalities and therefor risks. (Tam & Jones, 2019 b, 9-10)

Ship’s use GPS (Global Positioning System) for constantly updating information on position, time and date. The GPS is highly connected to other systems on the interconnected bridge. That makes it valuable to the ship and thus valuable to attackers. Moreover, satellite signals are rather easy to jam. (Tam & Jones, 2019b, 11)

Radar (Radio Detection and Ranging) signals can be jammed.

The NAVTEX-system sends information about weather forecasts and other navigational circumstances which may be of interest to the ship. It is a rather simple and non-connected system which means an attack to it would probably not cause critical damage. The main risks are false weather forecast information and updating via internet. (Tam & Jones, 2019b, 12)

NAVTEX is one of the GMDSS equipment which is required on-board ships to enable emergency communication. Other equipment are IMSO, EPIRB, SART and DSC. Some of them are autonomous and send signals automatically. By interfering in this communication system or part of it, rescue missions can be delayed or ships in distress unable to call for assistance. The biggest risk at the moment is installed malware. However, NAVTEX can also in the future be used for other purposes and be connected to the internet, as the connections get better (Tam & Jones, 2019b, 15-16)

As pointed out during this study, the ships are not the most digitalized workplace. The average age of the merchant fleet in 2019 was 21 years, with differences between vessel types. General cargo vessels’ average age was 26,4 years. (ICS, 2019). On the one hand it is a good thing; due to lack of internet connection and thus no external intruders. However, an isolated and technologically outdated workplace also leads to lack of knowledge and understanding. Furthermore long distances means challenges to keep hard- and software updated which results in unprotected and easily targeted systems. The internet connection and in particular e-mail with its malicious attachments and links, is a high risk. It is also possible that a personal device connected to the shipboard system causes a risk. (Tam & Jones, 2019b, 16)

Equipment for other than navigational and communication functions on-board may also cause a risk. Cargo handling machinery and mooring systems can be attacked causing damage. In its most extreme cases with automated cargo handling, attackers could also have the aim to steal cargo and remotely operated mooring systems can be interrupted causing collision with the quay. (Tam & Jones, 2019b, 18)

Risks related to information breach as described in chapter 6.4 and 6.5 may not cause direct impact on the ship's operation. They may, if the ransom or other demands are aimed at the ship or its crew. Apart from any financial losses related to criminal activity and damage to reputation, the GDPR includes obligations to member states for setting administrative fines for personal data breaches. Depending on the type of breach, category of data, level of negligence and other factors the fines can be set to

- 10 million EUR or 2% of the worldwide annual turnover, whichever is higher; or
- 20 million EUR or 4% of the total worldwide annual turnover, whichever is higher

To summarize; interference with shipboard systems can cause ships to deviate from its course due to false positioning data, avoiding an invented storm or other ghost targets on a radar screen. Company-related sensitive and personal data can be breached, as in any other organization handling this kind of information. The consequence is of course harmful to the individual(s) but also to the company. Criminals can require ransom and the company can face lawsuits resulting in significant fines if not all precautions have been taken to prevent a cyber security incident from happening.

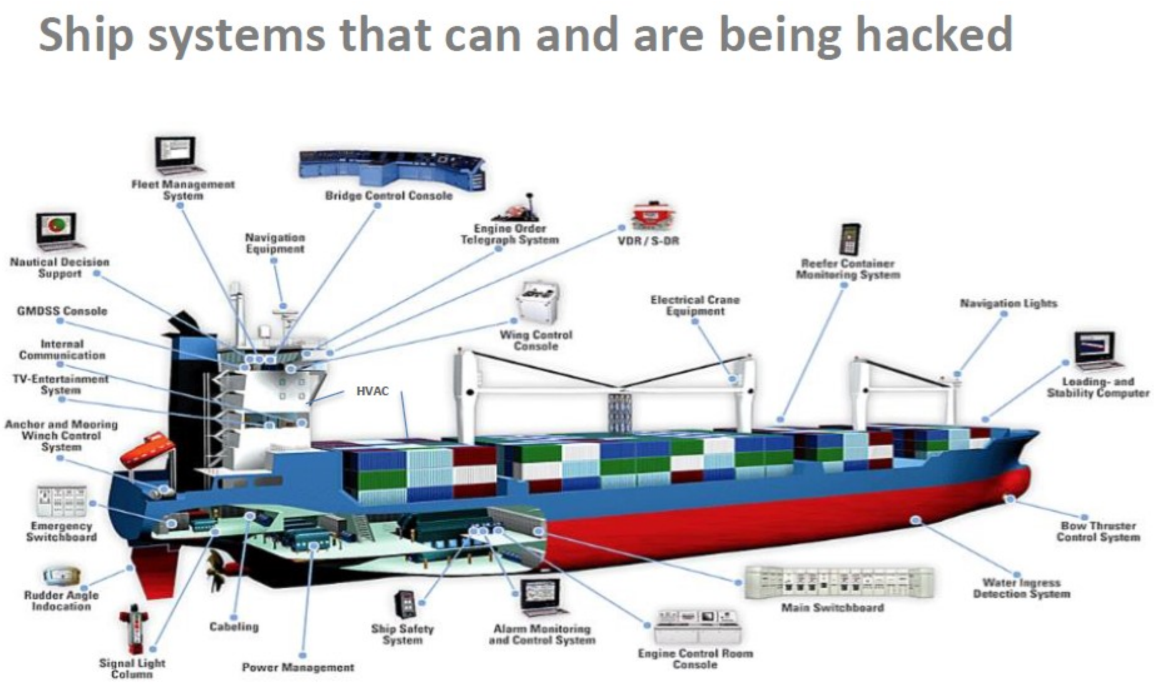

Ship systems that can and are being hacked
Fleet Management System
Bridge Control Console
Nautical Decision Support
Navigation Equipment
Engine Order Telegraph System
VDR / S-DR
Reefer Container Monitoring System
GMDSS Console
Wing Control Console
Electrical Crane Equipment
Navigation Lights
Internal Communication
TV-Entertainment System
HVAC
Loading- and Stability Computer
Anchor and Mooring Winch Control System
Emergency Switchboard
Bow Thruster Control System
Rudder Angle Indocation
Water Ingress Detection System
Main Switchboard
Cabeling
Ship Safety System
Alarm Monitoring and Control System
Signal Light Column
Power Management
Engine Control Room Console

Figure 10. From presentation by Dr. Christopher Henny, Brussels 18.09.2018

8 Cyber risks: ports

Finland is often considered to be an island due to its geographical location in the far north surrounded by sea in the west and south. Smooth and uninterrupted port operation is of very high importance for the transport of raw materials and products in Finland's foreign trade. On the east side there is Russia and using road or rail transport from there is not the most convenient possibility. The main connections to the rest of the world are thus by sea. The port of Helsinki is in normal circumstances one of the busiest passenger ports in Europe. The ports are an important part of the logistical chain in Finland and the main ports are often situated close to city centres. Depending on the accident and substances involved, such as toxic or explosive materials, the consequences could be catastrophic. A smaller port handling less interesting cargo loaded on smaller ships, situating further away from city centres and residential areas may not be of interest to criminals and hackers. Risk management need to be appropriate, as in every other case.

Some of the cyber security risks have the same consequences as shipping companies, such as breach of valuable information or personal data. Ships might possess information only related to its own activities, whereas the information in both shipping companies’ and ports’ systems often include stakeholders. The ownership of cargo and storage assets can also be complicated and thus the effects on a cyber security incident could be difficult to handle, in addition to significant financial losses. (Ahokas & Kiiski, 2017, 27)

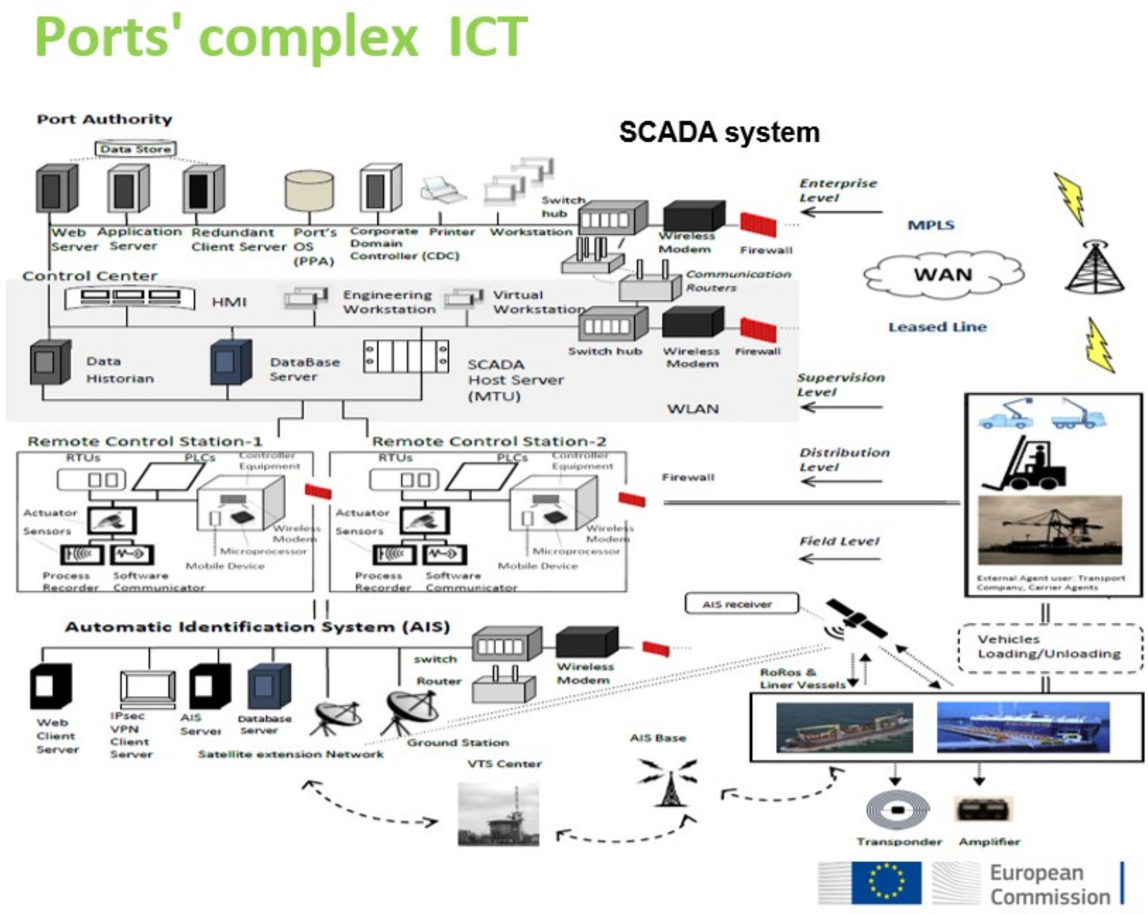


Figure 11. From presentation by Svetlana Schuster & Nineta Polemi, Workshop on cyber security in maritime sector, Brussels 4.9.2019

Cyber security risks related to port activities have been clearly listed by Drougkas et al. (2019, p. 26-27) in an ENISA report. Here we have mentioned some of them. There are many connections and integrations. There are information about cargo, vehicles and ships, it is all required in order to keep operations running. If there is a shutdown, there will be major financial losses. Interference with cranes, manipulating the flow of dangerous cargo or automated vehicles may even cause human injuries. A lot of personal and other sensitive data is handled by port systems. Containers may contain valuable cargo and information about them in the wrong hands is to be avoided. Container ships may thus also be attacked at sea, not in port, if the attackers receive information about ships route. Due to their location and important position in a nation's logistical chain, the ports' systems may hold information related to national security. As well as for shipping companies, also ports' reliability may suffer from cyber security incidents. Customers and stakeholders want their services to be handled by secure operators.

One specific risk, in addition to the general risks listed in section 6, mentioned in ENISA's report (Drougkas et al., 2019, p. 28) is related to access: brute force. This means that if a system allows using simple passwords, a large amount of attempts may result in unauthorized access to port systems. Similar to that, physical access can be granted for someone with a faked identity, also called "fake president fraud", where one uses a powerful person's identity to be given access. Taking the step to prevent an important person access might not be so easy in real life, especially if the person in charge does not understand the possibility of this kind of fraud. Deleting critical information is a rather simple mistake which can cause crucial harm to port operations.

Ports are very reliable on power supply. An interruption in the chain means significant slowdown or even stop, such as damage to good in refrigerated storages and loss of communication (Drougkas et al., 2019, p. 30).

In summary, we can state that ports are highly important nodes in the logistics chain, the vulnerability of which can be reflected in society as a whole. Furthermore, it is safe to conclude that the ports are part of our society's critical infrastructure which must be protected against intentional harmful conduct of any kind.

9 Cyber security management

A chain is only as strong as its weakest link. Voeller (2014, 29) sees a connection between this old saying and computer security due to the connectivity and integration. It is of crucial importance for people who operate in this safety critical work environment to have knowledge of the cyber risks associated with different operations and to understand the connections and consequences.

As in risk management in general, there is a need to focus on available resources in order to eliminate or minimize a risk in relation to the desired result. Therefore, in some situations we might be required to live with certain risks and settle for "being aware" or "doing our best". Most of us, whose specific task is something else than to keep the systems safe and secure, do put our data or systems in jeopardy in accordance to Voeller (2014, 41);

> "The net result of an unusable security measure is likely to be a system less secure than the one that started out as more insecure in the beginning."

We may have to accept that not all risks can be eliminated, at least not with a limited amount of work, time and to keep the costs in balance (Sales, 2013, 1503). It is important for companies to identify the most crucial systems and processes, prepare appropriate back-up and also decide which technical software or connections certain functions can live without (Fitton et al. 2015, 5).

We used three sources in order to find the relevant areas to be covered in the cyber security management, namely BIMCO et al. (2019), Mraković and Vojinović (2019) and Drougkas et al. (2019).

An industry driven set of guidelines has been compiled by a joint industry group led by BIMCO (BIMCO et al., 2017). It is quite extensive and recognizes five clear issues related to cyber security management: (BIMCO et al., 2017, 3)

- Identifying the roles => who has access to what and what are their tasks
- Identifying the safety-critical systems
- Implementing technical protection (such as access control, protective and detective software)
- Implementing procedures to be prepared (such as training, software maintenance, use of removable media)
- Implement procedures to identify cyber-attacks and to respond if one is discovered (minimizing consequences)

According to these guidelines, company plans and procedures for cyber risk management should be implemented to the existing safety and security risk management. ISM Code and ISPS Code are not providing enough guidance as they are now, their instructions are very general. Cyber security should be considered at all levels, from senior management to on-board personnel, as a part of the safety and security culture. Training and awareness is highly important to an effective approach to cyber safety and security. The internal cyber threat from own personnel is significant and should not be underestimated. The own personnel has an important role in protecting all systems but also a key role when it comes to human error aspects. Training and awareness should be given more effort. Shipping companies, ports and operators should be aware of the status of cyber security preparedness of their contractors and other providers. (BIMCO et al., 2017, 2, 25)

To conclude, BIMCO et al. (2017, 3) recognized five key elements: identify – detect – protect – response – recover.

Furthermore, Mraković and Vojinović (2019, 136-137) have divided cyber security management into sections covering the following:

- Human resources
- Technology
- Processes

These shall be covered in the management system.

The third source is ENISA's report (Drougkas et al., 2019), which uses the main groups

- Policies
- Organisational practises
- Technical practises

So, what does cyber security management mean in practice? In its simplest description it means being prepared, having agreed procedures for securing information technology, soft- and hardware and data from being damaged, lost or stolen. It is a wide concept.

As we can see, there are several different approaches to this. We decided to use the BIMCO-model, as it is more detailed and thus the terms explanatory. Next we will look closer into them. Chronologically we must first know what we have and who is involved. After that we can define levels and types of protection. Those things forms the fundamental basis and this lies in the hands of the management.

9.1 Identify

This is the most company-specific part of cyber security management. Size, location and connectivity of the organization, the amount of stakeholders, entrepreneurs and subcontractors involved in organizational processes are just a few factors which must be taken into account when identifying cyber risks. Persons and systems must be recognized; who is using what? (BIMCO et al., 2017, 3)

A security assessment can help the organization to identify the weak points, which is also the base for being prepared and able to recover, should an incident occur (Mraković & Vojinović, 2019, 137-138)

9.2 Detect

The basic fact for companies to understand when discussing cyber risks (other risks to safety and security, for that matter, but for the maritime industry those are a more familiar field), is that an incident or accident means financial loss. The amount, extent and time needed to resolve the situation depend on many factors and in many cases cannot be predicted. It takes time even for an IT-specialist to sort out the mess. Ulsch (2014, 77-78) has listed some factors which have an impact on the extent of the damage to business:

- The attack is not discovered. Technological protection is required, as well as observant users
- The company (users, IT-department) does not interpret signs to be an attack, which means no fast actions are taken to stop it
- After having discovered an attack, the company uses its own resources to solve it, which is unlikely the most effective nor fastest way
- Help from law enforcement is not adequate; the focus is on crime involved and direct financial losses (theft) but not the company's benefits on a more general level
- Management does not understand the risk of a cyber-attack; it is defined as a technological issue, not process- or human related
- Incidents are not reported. Companies are concerned about their reputation or afraid of being prosecuted for not having adequate protection
- Where external service providers are involved, they may not report the whole truth, which might leave gaps and unclear issues for the company to resolve in order to act responsibly

Where third parties are involved, focus on the service agreements should be put and the risks related to IT and information security identified already in the beginning of the cooperation (Ulsch, 2014, 154-166). The detailed information and separate issues to be covered will logically depend on the type of business, agreement and roles.

Organized crime can be the source to some of the malicious causes. There are resources and technological knowledge behind and the attackers may work for a long time before even discovering the attack. They know what they are doing and how to work without leaving tracks, which makes such an attack difficult to discover simply by raising awareness among the users. A frequent review of log data in the information system, such as a firewall, can expose such an attack. (Ulsch, 2014, 21-22) This information would be something a company's IT-department or at least a designated person would have and can make sure that proper check-ups are done regularly.

Daum (2019) has recognized the need for immediate actions within the maritime industry and has listed some cyber security measures related specifically thereto (Daum, 2019, 11-12):

- A responsible person for cyber security to be appointed
- Agreed protocol to prevent hackers from gaining access to IT-systems
- Early discovery of an attack
- Automatic action when an attack has occurred to minimize the damage

In Finland, we have a special authority for these issues, The National Cyber Security Centre that acts nowadays under The Finnish Transport and Communications Agency. This authority has a lot of good knowledge and material on their website. Most of the guidance is only in Finnish language, but anyhow very useful to promote the cyber security awareness.

A cyber security awareness handbook has been published by the EU (EU, 2017). It is built up with theory and a quiz in the end.

Best practices for cyber security on-board ships was published by the French governmental agency ANSSI (Agence nationale de la sécurité des systèmes d'information). It is a down-to-earth handbook with instructions for a basic internet-user, such as how to choose passwords and keep risks in mind when visiting different sites and clicking on links and opening e-mails. It consists of 34 pages, but only short sections and text on every other page. The best practices cover also private use, which could be forgotten when, for instance, focusing on instructing masters on how to handle personal data of their crew.

9.3 Protect

Technical devices as well as the networks connecting them or transferring data need to have adequate protection. As mentioned earlier in this document, high-level connectivity comes with advantages but also include new risks, unknown risks. It is, however, a new era of “normal” and something we should put more effort on to manage. An average user in a shipping company or in a port facility is probably not familiar with networks, connections and integrations and the risks involved. If an error or an attack hits one part of a system, what can the consequences be to another? The organization will need as much help as possible from technological solutions. Without going into detail, since we are not computer technology experts nor does this study focus on technological issues, we will in this section cover the most evident means of protective measures to equipment and networks.

A generally recognized challenge is that technology on-board ships is not the most recent. No approved updates are available to outdated hardware, which means the risk of using computer systems with inappropriate virus protection is evident. Ships have a long life-cycle, operate in a global environment and rarely need to have the latest technology, but some basic functions must be running. (Tam & Jones, 2019a) BIMCO et al. (2017, 24) state that computers on-board should have the same level of protection as in the office. It would be interesting to know how many shipping companies apply that guideline.

Wi-Fi networks include several technological vulnerabilities for a hacker to discover and use. There are ways to make security assessment, such as network sniffing (Salmon et al., 2017, 13-14, 21). In this work we will not look into various options to reveal weaknesses in companies’ own wireless networks. We have identified the risk and that there are ways to review the level of protection in order to take actions. The rest must be covered by IT-departments or outsourced specialists. As we see it, Wi-Fi networks can be used for work, at work; in office. Wi-Fi networks can also be used for work but outside the office-network. The latter is probably a risk recognized to some extent but do users understand it? The third type of wireless network usage would be for private use outside office network.

Hacking the Wi-Fi can have severe damage to a person in private. The IP-address can be used for criminal actions. (McDonough, 2019, 49-50)

At its simplest the system and software should be updated as well as the antivirus-program. Never add an unknown removable device in a computer. (McDonough, 2019, 67, 71-72).

Appropriate alerts and warning systems can help the crew on-board to realize there is something wrong with the system or its data (Tam & Jones, 2019b, 20).

Regarding e-mail, either it includes a link to be clicked on or request for money transmission, a basic rule is not to trust it (McDonough, 2019, 4). It might sound obvious. Nowadays most of us would not give our bank credentials or credit card numbers to a Nigerian prince so that he can release an additional 10M€ in return. But the situation is completely different when receiving a message you have been expecting, from someone expected and familiar, in a format expected and in between a hundred other things you have to get done by the end of the day, it is not so obvious anymore. There might be a contractor who needs a bill to paid in advance as in many cases before and you transfer the money as a representative of accounting department. Only this time it is a fraud.

There might be small indications, misspelling in the text or a minor difference in the sender's e-mail address, which might reveal the scam. If money transfer is involved, also double-checking instructions should be done. (McDonough, 2019, 4)

The most common attacks to individuals are phishing e-mails and malware (McDonough, 2019), two types of social engineering. It does not matter how technically protected the network or the devices are, if the recipient is unaware of the malicious intent. Users must be aware of the risk. No information shall be shared, no money transferred and no job offer accepted before having confirmed the validity of the contact.

Password control is highly connected to an individual. Devices or systems can, and should, force the user to choose a secure password with different characters. It is then in the user's hands to set different passwords for different accounts, such as private e-mail, web shops, Apple- or Android accounts and so on. If a hacker gains one password and the individual uses the same in more sensitive accounts with access to critical data (for instance social security information), the damage is evident. Every site which requests for your credentials when it should not, should raise an alert (McDonough, 31-32). An individual password for each account, preferably two-factor authentication, should be applied (McDonough, 25).

A cyber-security breach can occur also when being connected as a private person, either using company- or other wireless networks.

Ahokas and Kiiski (2017, 12-13) found three relevant questions to be answered:

- "From what are we protecting ourselves?
- What are we protecting?
- How are we protecting it?"

Having the answers to these questions helps the organization in their risk management. What equipment, networks, systems, connections and data are crucial?

Protecting an organization from cyber security related incidents includes both technical and operational measures. All employees must be included and aware. Crews on-board change constantly. Some return to the ship after weeks or months at home and some are one-timers. Any awareness program or checklist must be in the safety and security management systems in order to guarantee that everyone has received updated information about current systems, updates, dos and don'ts. Especially the don'ts.

9.4 Response and recovery

As the incidents is on-hand and has been detected despite all protective measures, the organization should have clear ideas on what to do now. The safety management system should include this. Loss of data, connections or being the target of a ransomware-attack require different set of immediate measures. The maritime industry is familiar with emergency-readiness and drills are arranged regularly. Cyber-related incidents are a new phenomenon, and it is important that the agreed processes are evaluated thoroughly, especially regarding the connectivity; if equipment is infected with malware, starting up back-up without clear understanding may cause another cyber incident. The next steps shall be available in non-electronic format. Response to a cyber incident shall include an assessment of the situation and damage, in order to get a complete picture of the consequences. (BIMCO et al., 2017, 31-33)

Incidents occur and we cannot be 100% protected from cyber risks. When planning risk management from this perspective, it is very important to be prepared and have processes in order to react when interruption or malfunction has been discovered. One part of this is to have clear descriptions on the connectivity; which systems and what data can be affected by disturbance in others? A contingency plan should cover this (BIMCO et al., 2017, 13) and a recovery plan shall include descriptions on how to get back to normal, or at least minimum to enable business operations (BIMCO et al., 2017, 34). Back-up allows a "fresh start", where lost or damaged information can be deleted and new data inserted again (BIMCO et al., 2017, 25)

The cyber world with its equipment, systems and connectivity is a rather new field for ships, shipping companies and ports to cover. Being safe, secure and protected does not come without a cost. Investing in cyber security management may not be something operators in the maritime industry are happy to do. One reason for this is the fact that so many different actors involved and the responsibility is shared between the company and the service-providers of its outsourced information technology services (Sales, 2013, 1508). This means that there is not only the workload added to the company, but it comes with a price tag. How can the human element -part be improved and risks minimized without unreasonable burden – and costs – to the operators?

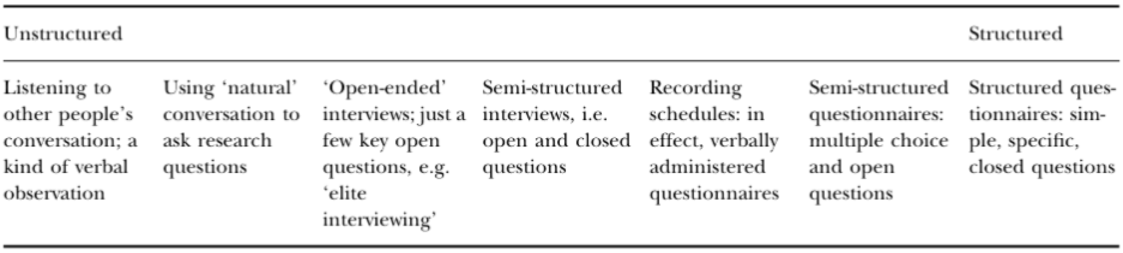
10 ISM Cyber Security 1.1.2021

The addition to the ISM Code regarding Cyber Security is a very present topic today since it entered into force on January 1st, 2021. It is the first and only global set of standards related to cyber security and therefore we have reserved a separate section to go through the guidelines before moving on to case- and field studies. The status of the document is strong recommendation and it does not in detail provide shipping companies with instructions on how to protect their information, technology and networks from failure or external attacks. As mentioned earlier, the maritime sector is a global industry. There are small companies with a few small ships who can operate without real-time updates between ship and shore. The trading area might even be rather close to main office, which makes physical contact possible. The ships may be small, not of the latest IT-standard and easier to operate even without a huge amount of sensors providing data. This reduces the need for high-level technology and connectivity via networks. Then there are bigger companies, working world-wide and the only contact to the vessels is digital. The ships are large, modern, automated and connected – also more interesting for attackers? The amount of workers is too big to control without having systems, databases and sharing information via networks. In this reality, it is crucial for the companies to be able to make their own evaluations and set their own standards as appropriate. The question is – do they have the capability to do so?

11 Case study

Questionnaires as such are generally not seen as the best method for collecting valuable data, especially when structured. The answers are chosen by the researcher(s) and the respondent will choose from them. A questionnaires with explicit options to choose from does not reveal if the respondent would want to explain why they chose a particular alternative or would like to receive more information about the particular question. They may not feel completely satisfied with the questions, nor answers which are presented to them instead of the other way around. (Gillham, 2007, 2, 4)

As described in the section 1.4 Methodology, we have decided to use a semi-structured questionnaire as a base for our interview.



Unstructured						Structured
Listening to other people's conversation; a kind of verbal observation	Using 'natural' conversation to ask research questions	'Open-ended' interviews; just a few key open questions, e.g. 'elite interviewing'	Semi-structured interviews, i.e. open and closed questions	Recording schedules: in effect, verbally administered questionnaires	Semi-structured questionnaires: multiple choice and open questions	Structured questionnaires: simple, specific, closed questions

Figure 12. Different types of questionnaires by Gillham (2007, 3)

Voeller (2014, 4-5) stated that organizations struggle with how to define their own level in being cyber secure. Depending on how computer-based, connected and integrated processes a corporation has, the more data there might be available. Companies might have too much data available to use as a measure or too little or simply choose the "wrong" set of data to make a review of their status. You must know where to look at and why in order to get the best conclusion. Voeller (2014, 5) mentions one specific example, which is understandable:

> ”if people are allowed to choose which measures they will collect and share with others, they are more likely to collect measures that demonstrate positive results (e.g. 100% of desktop computers have antivirus software installed) than measures that demonstrate negative results (e.g. 15% of antivirus software installations are up to date).”

We also feel that the shipping industry will not see the identification as an easy task. Computers, connectivity, integration and automation are rather new phenomena in the maritime industry and the operators might not have all knowledge required for such an analysis. This means the research questions are of importance. If the targets for our interview (responsible persons for maintaining systems and connections, setting internal rules and guidelines on how to work with computers, data, IT, transmitting of information) do not know what we are looking for, how can we expect answers and results to use in our study? Or we can even take one step back: if the users or company-designated persons to have overall control and management so cyber security do not understand connections, integrations and consequences of malfunctions in one end to results in other parts of the process, what is then the quality of data collected via our research? We must pay attention to the research questions and understand our interviewees; we should know what they know or do not know in order to draw any conclusions.

When developing our questionnaire to use as a base for the interviews, we used the theory and previous research from our study and recall the two goals for it:

1. To find out the general level of knowledge about cyber risks on-board Finnish ships and ports and the preparedness against them
2. to increase the cyber security awareness and to disseminate good practices.

Svilicic et al. (2019a) have developed questions when determining cyber security risks and cyber security awareness among the crew on-board. From that survey we were able to get some indications on how to prepare the questionnaire, even if the focus in that study was only related to ECDIS. (Svilicic et al., 2019a, 4-5)

Earlier in this study we looked at science of social engineering from a cyber security point of view. Simultaneously we also learned that in the role of an interviewer it is important not to interrupt pauses. There is a risk of filling in the answers or leading the interviewee towards a certain direction, manipulating. (Hadnagy, 2014, 12-13) As researchers we want information that only the interviewees can give us. It is of utmost importance and requires skill, to let them talk and keep it going without leading the conversation towards a certain answer. (Gillham, 2007, 3)

A face-to-face interview allow the interviewer to show interest by eye contact, smile and other non-verbal communication, maybe nodding. This encourages the respondent to keep on going without interruptions since the researcher stays quiet. As stated earlier, the interviews were not conducted in the same room, so other issues regarding behaviour during an interview, such as location in the room and physical contact, is not covered here. Gillham has listed some very important issues for us unexperienced interviewers to keep in mind: (Gillham, 2007, 30-35)

- Try not to be too anxious in getting answers. This usually has the opposite affect
- In the beginning of the interview the discussion may be slow, inactive. Do not rush. Give the interviewee time!
- Silence is ok – for both parts. It usually does not last for as long as it seems. Silence from the interviewer's part can mean that you are reflecting on what was just said = you were *listening*

Listening to the subject for the interview is the key. With only one researcher this is a challenge, especially in our case where we excluded transcription for reasons stated earlier. We are two, so one of us can make notes and the other one keep on listening. The interviewee can interpret if the interviewer has been listening or not as the following questions or supplementary questions come up (Gilham, 2007, 34).

When planning an interview, we start with topics and then continue to work on the particular questions; how should be form them in order to obtain information if value (Gillham, 2007, 19-20). We should also be prepared for sub-questions, called prompts, or probes, which are elements used to steer the discussion back on track, if it has lost its focus (Gillham, 2007, 14). To proceed to our data sampling from selected shipping companies and ports, we state that cyber security and cyber risks in this work covers the following areas which we will use as a base, not in order of importance:

1) In general: identifying the roles which can have an impact on cyber security in the company
    a) Who is involved?
    b) How are they involved?
2) In general: identifying technological equipment, systems, networks, connections and integrations

   a) If one system fails or is under attack => impact on other systems/equipment?

   b) Identifying critical systems

3) In general: use of service providers / third party vendors?

   a) What kind of services or processes and access?

   b) Background/reference check on the service provider?

   c) System integrations and data transmission involved?

4) In general: information technology tasks handled in the company

   a) By own department or designated "IT-guy"? Outsourced? Responsibility in the company?

5) Authentication of access to databases, which consists of two separate phases (two-factor authentication,):

   a) keeping updated information about user ID's and passwords to relevant databases, applications and information or even certain files

   b) verifying that the user actually is the designated user and not unauthorized personnel or external individuals obtaining information or being able to interfere with existing data for their own devious purposes

6) Authentication of physical access to buildings, offices, port areas, ships, designated areas on-board etc. Also this issue covers two parts:

   a) granting access

   b) verifying that the person when entering actually is the same who holds the right to enter the particular location

7) Social engineering (providing information to unauthorized persons with devious intentions)

   a) Physical contact (letting unauthorized persons inside offices or on-board ships)

   b) Phone calls (spoofing)

   c) E-mails and links to web-pages (phishing)

8) Preparedness for malfunction or attacks:

   a) Internal processes for reaction to abnormal behaviour of a system/equipment => how to discover a problem, when and how to react

   b) Back-up to guarantee no critical information is lost

   c) Resources ready to deal with the incident

With all of the above and previous analysing during this work, we listed as many questions as we could think of. We filtered and developed them into selected questions for our survey. The questionnaire is found as appendix 1.

11.1 Case study: Ports

Based on the workshop arranged by the Finnish Transport and Communications Agency (Traficom 9.4.2019) the greatest risk related to port operations are:

- Interruptions in the power supply chain, as it interrupts almost all activities
- Problems/malfunctions with the network, due to connectivity
- Problems/malfunctions in operational systems
- Cyber security awareness among own personnel

Sabotage, terrorism and other intentional damage are seen as s serious threat, but not as likely as the risks listed above. 9.4.2019 workshop materials are not publically available and cannot be attached to this Thesis. One of the authors (Henri Wallenius) was involved in organizing that workshop and this is how we have access to these materials.

As our scope focuses on the human element, we have looked deeper into the outcome of the workshop related to this issue. The intense working environment reflects to risk management in general. Time is limited, employees are busy and no extra hands are easily provided, which means it is a challenge to find someone to develop good practices and for the specific employees to implement and remember everything. There might not be enough knowledge about this area to start working on it not to mention the challenge with facilitating changes within an organisational culture. Furthermore the ports listed lack of knowledge and training to be a risk. This might cause intentional errors, which fairly easily could be prevented. In some cases instructions may be in place but they are not being followed. All-in-all, cyber security risks are not familiar to workers engaged in ports. We are not prepared for what we do not know or understand or identify as being a risk which could cause damage.

Social engineering, phishing, spam, malware, data breach are some typical cyber risks which the port operators identified. These are the same as for shipping companies.

In order to cross-check the findings we also checked ENISA's report from 2019 (Drougkas et al., 2019, p. 30-31). The human element -related challenges identified are more detailed compared to the material we used:

- Lack of awareness and training
- Lack of digital culture – the challenge with implementing new technology in conservative environments, which is the same as for ships. Maritime industry has a long history and thus is not yet familiar with all the new technology in comparison with other business areas)
- Lack of time and budget reserved for cyber security -related improvements
- Lack of human resources and knowledge to make required improvements

11.2 Case study: Shipping companies

As previously explained, we surveyed the views of the shipping industry through direct interviews. This section explores the insights gained from these interviews, the questionnaire used in these interviews is attached (Appendix 1).

We explained to all interviewees the purpose of our thesis and how we intend to report the findings of these interviews. We wanted to emphasize the confidentiality of the discussions and the fact that all material is treated anonymously. All interviewees were company security officers (CSO) and designated persons (DPA). In the following part we will "unpack" the results of the interviews question by question (Questions 1-13).

Question 1:

We started the interviews by seeking clarification on key terms; how does the company DPA define cyber security and cyber security risk.

Cyber security was considered to be a broad term. It includes a lot of things, both information and technology. One response was (translated from Finnish):

> "Cyber security means control of data transmission"

Furthermore this particular respondent explained that orders might come from ashore to the ship or vice versa. If remotely operated, cyber security means to keep the data transmission protected.

Cyber security was explained as how we use information technology equipment and how we use and save the data. It was recognized that computers play a major role in our working environment. In the future, when ships may be remotely operated, the interference in transmitted data can cause severe damage.

The ECDIS-system was recognized as a critical system on-board. If a virus gets into it or someone from the outside can control it by changing routes, the consequences can be severe and this is identified as a cyber security risk.

In general cyber security risk is identified as a threat from the outside, something causes interference to our systems or data:

> "Someone else is in control of our systems"

A technical malfunction can enable an attack to the systems. Furthermore, data breaches were mentioned by all of the respondents. Data in the wrong hands is a risk. Some also mentioned not only personal data but data related to contracts and cargo, e.g. business-sensitive data.

One of the respondents wanted specially to bring up the fact that in media and general cyber security discussions, cyber security risks are mostly considered to be caused from the outside. In this case the respondent wanted to define also errors and bugs, even physical such as a disconnected cable.

Two of the companies also wanted to emphasize that risks and thus preparedness for them can be different from company to company and depending on the ship type. New ships have in general more advanced technology and are more connected than others. Some ships have valuable cargo while others do not and are not an interesting target from that point of view. The variety among shipping companies and need to take appropriate measures are evident factors. We have recognized and mentioned that previously in our study.

Our definitions as we described them in the beginning of this study:

"Cyber security means protection of data, technological instruments and assets. It includes the human element, the users of the information, technology and applications and networks. The humans can be tricked or manipulated in different ways and on the other hand, they can be the heroes when protecting their ship(s) and company from disaster or minimizing consequences"

Cyber risk:

"An unwanted incident, deliberately caused or by unintentional error, which may cause damage or malfunction to a company's information technology systems, networks or cause data breach."

We can conclude that the interviewees share our view; they identify the equipment, systems, network, data, the human element and the possibilities for both intentional attacks as well as undeliberate errors. However, in some discussions it came up that the difference between "normal malfunction" and an attack caused by an outsider, is not clear. Those are difficult to identify for a normal user. Nevertheless, any technical malfunction to an IT- or OT-system should be handled as a cyber security risk and proper back-up should be arranged regardless of the cause.

Question 2:

Our second question was about security gaps in general. Here we made it clear to the respondent that we wanted a general view in the maritime sector, not in their own company.

A general opinion was the human role as the user; do the users understand cyber-related risks? When ordering service to equipment, systems or applications, do we now what can happen and how we should protect what? Technology evolves faster than the users gain knowledge.

USB-sticks were mentioned and some companies, not all, had instructions for using them. In other words, guidelines on NOT to plug in unknown devices into those computers which are used for business purposes and connected to other equipment.

Another interesting observation were the ship-specific systems. Personal computers, the applications and e-mail programs have firewalls and antivirus systems installed but what about navigational and engine room-specific systems and connections? There might be gaps, as one respondent was thinking.

Protecting data, especially personal data, might need improvement. If data is stored in different places, it is more difficult to handle. Smaller shipping companies may have excels to store data and medical certificates on hardware.

Newer ships have more advanced technology, as the respondents reflected, and this means more advantages but increases risk for gaps in the cyber security. Data is transmitted to manufacturers in order to serve the customer (as an example was mentioned new car automatically ordering a new set of tires and then informing the owner by e-mail) and to develop their own technology. Do we as a shipping company even know what data is being transmitted and to whom, as one respondent speculated. The general view here was that technology evolves faster that we as users or managers are prepared for. How can we protect ourselves from what we are not aware of?

Question 3:

Next we wanted to dig into the specific company represented by the interviewee. We asked them now to consider their own organization and lift up the weak points in the field of cyber security – where is room for improvement?

The human element. Lack of knowledge, understanding, plugging in own devices, share internet from a mobile phone, which in one case had resulted in malware to the system. Another company had got a virus from a USB-stick and the computers and systems had to be cleaned. One company pointed out lack of access control, which has not yet been clearly defined. Who has access to what and how do we manage that?

Ships sail to different ports and sometimes in a foreign port there is a need for updating something or more likely, a surveyor or inspector asks to print some documents from a USB-stick. The step to refuse in order to prevent possible virus spreading to the system, is not so easy to take on-board.

Virus protection and firewalls were in general considered to be adequate. But as stated earlier in this study, not even the most efficient protective measures can prevent the user or an external source from causing harm, intentionally or unintentionally.

Some companies do not have separate computers with possibilities to define work- and civil use. Some do and in one company they have clear instructions regarding which computer is only to be used for work. However, the respondents reflected, we are not 100% aware of how the instructions are being followed on-board. In addition to knowledge and understanding the attitude is equally important. We in management must be committed, understand the importance and share this within the company.

Question 4:

We asked if the company had encountered cyber security attacks. The answer was: yes. Spam and phishing e-mails were familiar to all of them. We could see from the answers and the difference between the companies that some have faced more than others and that, based on our study, the ones who had faced more of them also had been able to stop them. Conclusion: they might be more aware and thus recognize attacks better than others and also be better prepared. They may also identify being a more tempting target and that is why they encounter more attacks and have been better prepared. We cannot draw a 100% conclusion without further investigation.

Malware sent in a link in an e-mail had caused a virus to the computer. This has happened to more than one of our respondents. Clicking on a link or open an attachment too quick can cause this. Some companies had better spam-protection than others, as can be concluded from the discussions.

The conclusion here is that attacks via e-mail are familiar to all shipping companies. Some are targeted more than others, some are better protected and some do not recognize the attacks and are lucky. E-mails containing rewards or requests from the managing director to quickly transfer money were also recognized by all of our interviewees. These were, however, well identified and had not caused revealing of requested data nor money transfers.

Questions 5 & 6:

The nest questions were about how ICT responsibilities and tasks were organized in the particular companies. The DPAs were all very well aware of responsibilities, which is no surprise as the safety management system obliges them to have overall knowledge. Some of them had IT-departments and most of them had outsourced some of the IT-related tasks, such as service and support.

Question 7:

When asking our interviewees about the implementation of cyber security in their own safety management systems they were all considering the recommendations as mandatory. As we wrote earlier in this study, the statutes from the IMO are still recommendations. They were all aware that on the first office audit after 1st January 2021 this should be covered. They were all working on it and two companies had it quite thoroughly covered already; one company had had the first audit already in January and another had already for a couple of years had a separate section in their Safety Management System. All of the respondents had a positive approach towards us contacting them at this stage, as the work is under progress and by asking questions, we reminded them and in some cases also developed new aspects on these issues.

Question 8.

Some of the companies were working on the risk evaluation related to cyber security. One company which had done it already, had resulted in a requirement for a work permit for all IT-related work on-board. Basically, if an external service provider comes on-board to fix something, it requires a permit and there is a clear process for that. This also helps the seafarers on-board to be aware and vigilant. Another company had done the analysis at a general level, including measures when something happens. The interviewee felt that it could be more thoroughly analysed considering the most likely threats to their specific company. All companies were well aware of making an evaluation and how to deal with identified risks.

Question 9:

We asked the DPAs how likely they estimate a cyber security incident is to happen. There were differences here, some said “not very likely” and some answered 4 on the scale 1-5. The arguments were good from all of them, and here we can see that the ship type, trading area and the age of the vessels have an impact as well as what is considered to be a cyber security incident.

One comment was that the maritime industry is a little bit behind and has not been discovered by cyber criminals just yet. Here was also a reference made to the globally well-known "Maersk-case" (This giant shipping company was hit by the so called NotPetya malware in 2017).

However, as all of the respondents had encountered phishing e-mails, the likelihood for someone someday to open a malicious attachment causing a virus in the computer, we would easily have thought that they would all consider the risk to be “very likely”. One company also responded that if all e-mails, also those getting caught in the firewall- and other protective systems, are considered, then we are being hit all the time. On the other hand, this incident may to some companies be caught and in others, even if activated, only cause damage to that particular computer due to no connectivity. Thus the company has evaluated the damage to be so small and thus not even consider it to be a big risk. Others may be more sensitive and define all cases as “incidents”.

We also must remember that size matters; a company with 200 computers and 1000 employees has a larger likelihood to be hit than one with 20 computers and 100 employees. The employees are more difficult “to handle”, which here means to train and instruct. In bigger companies also the turnover rate among employees tend to be larger.

Questions 10 &11:

At the end of our interview we wanted the shipping company representatives to evaluate the cyber security awareness among their own employees (on-board and ashore) and also whether they have organized drills and exercises in the field of cyber security.

The responses were: two companies: low awareness, one company: high awareness and three companies: medium awareness. However, we had only given the alternatives “high” and “low”, and the first interviews strictly chose of those two. At the end we added the possibility, via discussion, to also choose “medium”, so they cannot be completely compared. During the discussion it was evident in all cases, that some employees are more aware than others.

Some seafarers have received their training in the 80’s or 90’s and no updating training taking these issues into account exists. Even if their education is from the 21st century, the maritime training is based on international standards and as clarified in previous sections, the development is slow. The companies recognized different needs on different ships and varieties in knowledge: in general younger employees are more aware than older ones. When bringing up the awareness and understanding, all shared the same opinion that training is needed. None of them had arranged specific drills related to this. One company sent out e-mail disguised as from a high-level-manager. This can be seen as a drill and the result was that many people did not pass.

One response to the question about arranging cyber security drills was: “It hasn’t even crossed my mind!”. When reflecting over this, together with the interviewer, they all had a positive approach and realized that a “cyber security drill” does not necessarily mean a separate addition to existing training manuals and programs, but can be included as a discussion-based addition to existing drills. At a minimum one could bring up the topic as a reminder. One company regularly sends information, warnings, about specific phishing-mails attacking the company. This happens on a weekly basis and can be seen as some kind of drill or training.

Question 12.

There were variations between the companies on internet-usage on-board; some have separate computers and also separate networks for private and business use including instructions on how to use them. However, even in the cases where proper instructions were in place, the respondent was not completely convinced that the computers and networks are used as appropriate in accordance to the given guidelines. Some functions were blocked and better protected but others had only user’s guidance to rely on.

Question 13.

Last but not least we asked for comments about the interview, the questions and if the interviewees had something additional they wanted to share. Ordinary software failures and malfunctions, physical malfunctions (cables and fuses) or failures in the operational systems causes risks to everyday ship operations. One of the companies had not during the last three years encountered any hacker- or other incidents related to criminal activity but several malfunctions each year. Authors’ comment: do they know for a fact that there were no outsiders involved in the system errors considered to be “general malfunctions”?

In general, we received positive feedback. The timing was very suitable. We had given them a reminder and even some good points to think about during their work in implementing cyber security into their safety management systems. The future will certainly bring us ships with a higher level of technology and if automated or remotely operated ships emerge (there was some scepticism among the respondents), the cyber-world must naturally be much more under control than it is today.

12 Reflection on research

Analysing the qualitative data in order to make conclusions is a difficult task. We chose to follow Walliman's advice to keep thorough notes, write down as much as possible immediately during and after the interview when we still have something stored in our memory to use. Furthermore the idea was to write all collected answers and comments in similar format. (Walliman, 2010, 132)

During the whole interview we had the questionnaire visible for the interviewee. This way they would not lose focus on what was asked and they could go back, reflect and conclude. The interviews were done using "Skype for Business 2016" software. The interviewer shared his desk top with the interviewee displaying the questionnaire. We felt this was a good strategy.

An advantage of being two involved in this survey is that there are more ears listening and hands writing so we can support and complete each other's notes. The work when analysing and putting all on paper was also easier, we think, as we did it within a few days after the interviews and together were able to discuss findings also from our memory based on the notes.

When asking to describe terms “cyber security” and “cyber risk” we noticed that not all subjects answered the question “cyber security”, and focused only on “cyber risks”. This would probably have been avoided by clearly separating the questions and not combining them. However, as both terms are related to the same thing, it did not have an impact on the result. If “cyber risk” is explained, then “cyber security” would mean avoiding that risk. This is a good example on how to avoid too long answers or actually not receiving a clear answer. Lesson learned: do not combine several things in one question.

In the first question regarding explaining the terms we also discovered that one respondent had focus on remote operations, probably due to our study programme which we explained in the beginning. Maybe we could have asked for an explanation but as we wanted to be very careful and avoid leading the interviewees on, we did not ask nor comment. Neither this answer had an impact on our overall result, as it later in this interview became evident that also this particular respondent talked about the situation as it is today and not maybe in the future. Lesson learned: be more specific if there is a risk that the context for a particular term or definition is not 100% clear.

When defining cyber risks, we discovered that also bugs and errors were identified as “normal malfunction” among the respondents. However, some malfunctions, intentional or not, random or aimed attacks, may also be a result of a cyber security attack. It is very difficult as a user to identify the cause. The dispatched cable will most likely be identified and discovered but not the information technology- or operational technology-errors. This also can be a consequence of the cyber security protective measures in a particular company; we discovered that one company, which had very effective firewall-, antivirus and spam-protection, had not encountered attacks or attempts (as reported from their IT-department), but normal malfunction was a very general issue. Are these malfunctions just part of the technical systems or could there, in some cases, anyway be an attack behind? We did not dig that deep and as we did not interview IT-departments but operational managers (CSO / DPA), we do not have answers to this.

All respondents recognized the different profiles among companies and felt that passenger vessels probably are more attractive targets than general cargo. However, some attacks are random and cause damage to the weakest link. The least protected target is found regardless of the value it leads to. The already previously mentioned and commonly discussed Maersk-case was recognized by all respondents and that is one example of a randomly aimed target to result a huge amount of financial loss.

The question regarding experience of cyber-attacks resulted in interesting answers: as they were described to the interviewees (malware, spam, phishing, social engineering etc.), it turned out they had experienced them. First we were a bit worried that this would lead them on – we are putting answers ready – but during the interview it was evident that if we had not defined some of them, they would not have been recognized as “cyber-attacks”. Maybe some other general kind of sham but not particularly cyber-related. This was the feeling we got during the interview. Lesson learned: if the field of research is new, as in this case, it may be good to add some more information into the question. Not all extra information means “putting words in their mouths”.

The timing for our interviews turned out to be suitable: they were set for beginning-mid April 2021. At this time all of the companies were working on implementing cyber security issues into their company ISM-systems and us contacting them was a positive thing. They were reminded about this work and also got some new points to reflect. When conducting a case study, the information received is very important. If the interviewee is not committed, the result will probably not be as qualitative as hoped for and thus not of value. We feel that one of the goals of our Thesis was met through these interviews, namely raising cyber security awareness.

13 Recommendations

Lack of cyber security knowledge is a fact in the maritime field in Finland. Our respondents during the interview as well as the discussions from the cyber security workshop arranged with the ports in April 2019, showed that the management has acknowledged this state and that improvement is needed. The interviews also revealed the general feeling that the situation would be rather similar, if not worse, all over the world. The ships operate in a global industry which logically means a high variety of companies, ships of different ages and thus levels of technology as well as differences among the seafarers.

Ships, shipping companies and ports already struggle in a jungle of regulations, laws, documents, processes, checklists, audit systems, inspections, certificates and familiarization and training requirements. It is of utmost importance to have a balance, even though a gap has been discovered. Adding more requirements, guidelines, recommendations and setting new internal process-requirements may not as such result in higher level of, in this case, cyber security. We see that the international guidelines should be made mandatory, short and clear, and leave the implementation to the companies and ports in accordance with their own level of equipment, technology, number of computers, users and connectivity to mention a few aspects.

In our study we aimed to look into the human element. Therefor our conclusion in the recommendation for improvement based on the findings will also be linked to the employees. Next we will suggest a training program for shipping companies and ports to develop, in its simplest form.

13.1 Cyber security in company management

The responsibility to have also cyber security covered in a company's safety management system lies on the management level. In real life, there is only so much we can expect from the user, in this case our employees on-board or in port operations.

The key elements, as presented in section 9, are:

- Identify
- Detect
- Protect
- Response and recovery

Furthermore, the areas to be covered are human resources, technology and processes. In our study we focused on the human element.

In its cyber security assessment the company shall identify who has access to what and what functions they are authorized to perform. Keeping the access control updated is of crucial importance, not only from the personal and business-sensitive data protection point of view but also to minimize the risk of intentional damage caused by ex-employees, for instance. If processes are outsourced, the control is even more important.

The company management must be committed and understand the importance of cyber security. If incidents are interpreted as purely technical, corrective measures cannot be taken to prevent similar events to occur again. Management together with IT-department should find key elements for employees in different roles to themselves be able to identify cyber incidents and attacks. Detecting the incident is, of course, crucial in order to solve it.

Protection includes technical preparedness; anti-virus systems and firewalls, as well as process-based: forbidden usage of removable devices and private mobile networks in systems meant for professional use or connected thereto. The company management must make sure that the hardware and software are installed with proper protection and that they are updated. Proper precautions also in this context should not be forgotten. What to do when a normal procedures or systems are not available, must be planned ahead. Well-designed preparedness is part of safe and secure shipping operations.

13.2 Company-specific cyber security training

As mentioned earlier, we understand that not all risks within reasonable resources and efforts can be eliminated and that the level of protection must vary between companies. McNicholas (2007, 369) presents an information security function in a company where the highest level would consist of Chief Information Security Officer, Information Security Officer and Information Security Engineer. Even though these could be workers with other tasks and not be full-time security officers, it is evident that the average Finnish shipping company would not welcome this heavy organisation just for cyber security issues. In order for this responsible person to achieve desired outcome (higher level of cyber security and cyber security awareness), we also see the importance of this role to be familiar with the profession and work on-board.

People are lazy, we tend to take the easiest way. If our main task is something other than maintain the company's information and technological equipment intact, we will not put effort on updating antivirus-programs or creating complicated passwords which makes access to all the systems we use on a daily basis more difficult and time-consuming. There must be relevant protection level and simple processes to guarantee adequate use of technology, storage of data and transmission of information. How many of us have not clicked "yes" and "allow" when unidentified pop-up-windows appear while we are browsing the internet and the pop-ups keep disturbing us visiting sites we have no reason to suspect. These warnings have become a part of normal activity and as long as nothing happens, no consequences or data-breaches, we tend to continue doing just that.

BIMCO et al. (2017, 26-27) have listed some issues to be covered in a training for the shipboard crew, here some of them:

- Handling of e-mails and risks related to internet in general, unprotected sites and social media
- Connecting personal devices to shipboard network and level of protection (anti-virus) on own device
- Installing software or updates to devices or systems on-board (via verified links or removable media)
- How to handle user information and credentials

- Cyber risks caused by external persons on-board and the need to use shipboard systems – are they and their tasks verified? Can we allow plugging in their removable media?

- How to be suspicious and as soon as possible detect that something is wrong with a system or its information (slowness, errors, being locked out, systems crashing and other abnormal functions)

- Understanding how to technically be protected from a cyber incident (updated firewalls, anti-virus systems and proper back-up) and the consequences of one

Relevant security awareness familiarization and/or training is an obvious means of protecting a company from security risks. The questions is: *what is relevant and for whom?* The high-level learning expert, Professor Art Kohn, has done some research within the field of learning and memory. An interesting article from 2014 presents the "forgetting curve" and states that after having participated in a training, within one hour 50% of the information will have been forgotten. Within 24 hours, 70% and within a week 90%. If we want something to change, which usually is the fundamental aim for training, the participants must *remember*. There are various reasons for how the brain works and why it needs to filter some input. We are not interested in why we forget and training for that reason is insufficient. We would like to have a closer look at how we could decrease the forgetting-percentage and increase the probability of providing new information, relevant and important information, which will actually add value to the company. (Kohn, 2014)

There is a wide range of trainings available today. Theoretical, practical, in-class, e-courses, familiarizations and workplace-specific trainings. We should acknowledge the fact that there is a high risk of information overload and training tiredness. Adding new training into a shipping company's ISM-system or internal training manual does not guarantee any results. The training, in this case cyber-security-related, should first of all be recognized as *important*. This is something the company itself must figure out. The involvement and commitment of management is important. The emphasis on risks and important processes is different depending, among other things, on the size of the organization, its vessels, vessel types and ages, level of technology and connectivity. Once the importance has been recognized, the training as such can be planned. The most important thing is to make sure that the participants are forced to reflect, repeat and be reminded of what they have just learned. In short, this means that when their memory is used, their brains will consider this new information to be important and is not as easily lost (Roediger & Brown, 2020). So, there is a very logical reason for workshops during classes – students discuss, argue, reflect, dig deeper, write and talk about the new information. Simply going through the material, like rereading, does not give a better result. The twist is to reflect, dig deeper and see same issues from different perspectives, explain it in your own words and not only repeat the exact same wording. Quizzes, as well as asking questions during and after the particular training, have a better effect in keeping the new information in our minds (Roediger & Brown, 2020).

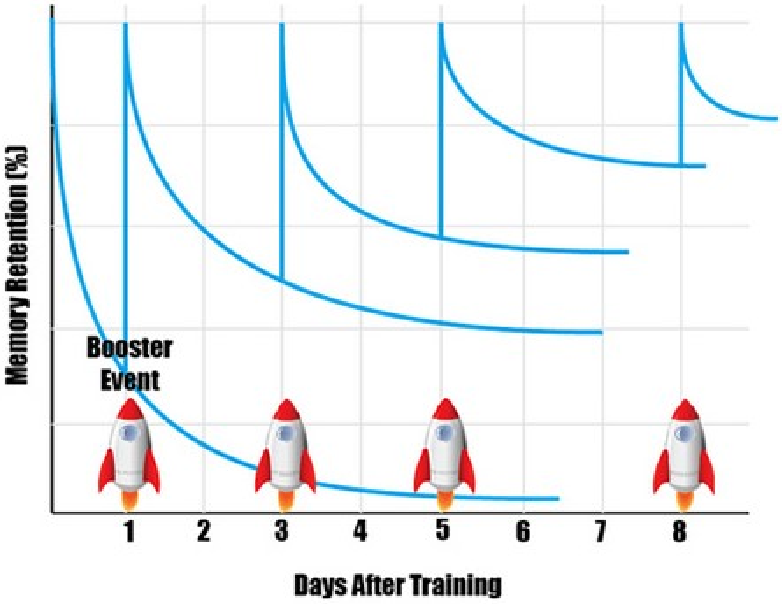


Figure 13. Visualizing the “booster events”, which flatten the forgetting curve (Kohn, 2014)

The maritime industry, in particular the seafarers, are heavily loaded with regular training requirements at training centres and things to take care of and have under control when at work such as ISM-related documents, manuals to read and try to remember, employment contracts and existing familiarization and drill requirements. We must keep in mind that these are not the employees core functions, which have refresher training requirements of their own, but shall be seen as support and aim for as safe and secure ship and port operations. In order to achieve goals and increase awareness, the process must be set to a minimum amount of work and resources and keep the most important issues in focus.

The management and office-staff also have their hands full when planning all these trainings and keeping ISM- and other documents and certificates updated. We must understand the context and try to keep this simple. In-class training would probably from the learning-perspective be the most equivalent alternative (Jaf et al. 2018, 4991-4993). Company-specific cyber-security trainings will include sensitive data and that would support the idea for arranging the training on-board, in person. However, as the information overload when boarding for the first time is evident, one could argue that delivering this training in electronic environment before boarding, could have a higher possibility for achieving desired results, which in this case means a higher level of awareness. Many seafarers have employments contract only during the time on-board and not permanent contracts covering also their days off the ship. Larger shipping companies have high levels of turnover among the employees. We must be careful who we share this information with. The training should thus not include company-sensitive data. Our study has shown that general information about how to use and protect systems and connections is relevant and an e-learning program (short!) which aims to increase awareness, can be done at a general level and still be appropriate.

As we know, information received from training is easily forgotten. A thorough in-class training, no matter how fascinating the lecturer or how interesting the subject, inspiring the surroundings or how focused the students, after one week they will have forgot 90% (Kohn, 2014)! To keep the issues in mind, cyber security-related matters could be added to the familiarization. This is also something which must be considered by a company- and even ship-specific basis. Some smaller ships have one new person signing on at the time, which means it is easier for the shipboard manager to explain to new employees what is relevant from *that specific worker's* perspective – who has access to what information technology equipment and data on-board. Some ships have several to be familiarized at the same time. The important thing is, however, to bring up cyber security and its importance when the new seafarer is boarding. It is easier to implement the right processes from the beginning than changing the behaviour of an existing employee. In Appendix 3 we have listed some questions and comments which can be used by the shipboard personnel during familiarization.

The computer-based training could be interactive with responses to click, explanations if something went wrong, pictures, videos and so on. It can also be a document including company policies and procedures to be reflected on as the person signs on. Such a document, at its simplest, is presented in Appendix 2. The important thing is to have shipboard personnel included in the development process in order to achieve an appropriate model. We who work by our computers all days long may have a different view on how much time and effort could be put into this than those on-board, so we must include in order to achieve the most appropriate model for that company, port or in some cases maybe even ship. As mentioned, shipboard work including computers, systems and connections shall support the seafarers in their core functions, not cause extra workload. When explaining what damage and extra work malfunctions, viruses not to mention interference in ECDIS-system can do, the target group for cyber security training will probably be more receptive to cyber security -related information.

The combination of face-to-face introduction on the subject and a computer-based part is also supported by Jaf et al. (2019, 4993). They have created a learning program with an onsite trainer and a computer-based part. The e-learning part included defined tasks that the user was supposed to perform – log in to Facebook, log in to e-mail, leave the computer for five minutes and execute an exe file. When performing these tasks, informative pop-ups occurred to provide information about e.g. company policy regarding social media (Jaf et al. 2019, 4998). The focus in this study was on social media.

To get some basic information one can use sources on the internet which are aimed at regular citizens. Our target group are "normal workers" and basic users of information technology systems, e-mail and social media, so any general knowledge will probably suit them, too. We think that governments apply mostly the same instructions for their citizens and decided to use guidelines from The National Cyber Security Centre of United Kingdom. It is evident that the availability of relevant information in English is at the highest level.

13.3 Motivation

To gain achievements, results and commitment from our employees, which are in focus here, we must understand their work environment. A passionate "IT-guru" who is focusing on his/her field of interest will not gain the respect nor support from the seafarers or employees in port, which makes implementing new or changed cyber security -related processes even harder. The development work, building a new field of security to be covered in existing management systems, need the view of the employees. Engage them in the implementation process. A well-founded and understandable goal is easier to achieve.

If people do not see the importance or value in something, they tend not to put effort in such tasks. Low interest is an extremely poor breeding ground, there must be proper motivation. Cyber security with its invisible threats may just be such a low-interest issue, at least for some people. One option is to add supervision and audits. These are familiar to the maritime sector already. However, employees also tend to prepare for the audit and in between, processes may not be fully implemented as they should, even if the management system says so. In such a case, the company has not succeeded in implementing safer processes to minimize risks caused by the human element.

Encouragement and reward systems are more positive ways to achieve goals. In normal working tasks show of appreciation, a simple “thank you”, “good job” and regular salary, possible increases now and then are plenty enough. When it comes to more difficult and less interesting tasks which do not add value to the core tasks, the employee needs something more to keep on going. Some kind of rewarding systems could be introduced to keep following cyber-security related regulations and internally agreed processes. Very helpful is also to get some interested and active employees to act as “agents”, since behaviour and setting examples usually has a positive impact on the others (Li et al., 2016, 109-110). Hopefully not everything needs to be learned through accidents and incidents, but through awareness raising.

14 Further research

We decided to have a rather small and detailed scope in our research. In the beginning we stumbled on clear cyber security -related risks which we needed to leave out in order to keep our work in control. The field of cyber security as such is rather unfamiliar to the maritime industry. New technology is evolving at a high speed and how to keep up with it (unless IT is your core business), is a challenge.

We had more focus on the shipping operations in this work, as the general opinion was that ships are a more heterogeneous group and the ships are in constant movement and not so easily upgraded or controlled. Ports are ashore and can be managed in a similar way as organizations in general, even though the logistical chain in itself requires people and vehicles passing through, constant access control management, connectivity and employees involved in very different tasks in different locations within the port area.

Hired employees, part-time or full-time, permanent or as contractors, this type of persons have gained the company's trust via their position and have access to facilities and data. We must acknowledge this group of persons as a possible threat. (Ulsch, 2014, 6-7)

Shipping and port operations go together, forming a very important part of the logistics chain. We believe that cooperation and a common vision on cyber security development is important both for the shipping companies and for the port operators.

Cyber security goes hand in hand with technological development. Increasing automation brings new challenges related to cyber security. Automation experiments and remote control projects open up new research needs in this field.

In addition, based on our research, we can recommend that cyber security education should be included in maritime training programs. Such a future study could include an assessment of the current situation on different levels and an assessment of future needs.

As the shipping business moves towards the expanding use of automation as well as remote control, we see that significant attention needs to be paid to cyber security. We see that this opens up many research needs and possibilities.

15 Conclusions

The implementation of cyber security risk management is ongoing among the shipping companies in Finland, probably also in other countries as the recommended deadline is first annual verification of Document of Compliance after 1st January 2021. In other words: the first company audit after that date. As the companies at the moment are going through their equipment and connections, authorizations and access on-board, the company will detect their own critical systems and what to focus on. We must also keep in mind that port operation are not in the scope of this regulation update.

Regarding cyber-security awareness training we conclude that:

a) Management must be involved and acknowledge the importance in order to communicate and show the organization that we are all committed

b) The training should be company-, maybe even department- or ship-specific or both

c) The training should be relevant and include quizzes or some other form of reminder – as a minimum immediately after the training and to repeat as appropriate

d) The training should be conducted before boarding as an e-learning and brought up during the familiarization in order to be available for all new employees as soon as possible.

As the old saying goes: "A job well-planned is a job half-done". The aim with the security training is to *increase awareness*. The name "training" shall not cause stress of yet another addition of classes and manuals for the ships, ports and companies behind them. If developed together with representatives for the target group, for whom the training is aimed, and made at company-specific level, it should improve the level of cyber security within the maritime industry in Finland. Keeping the training separate from other trainings and to be conducted on-line, also makes it more likely for the participant to focus and store some of the information. The familiarization, which is an ongoing process on all ships due to STCW-requirements, would include cyber security and reflect on what they have learned or in general what they know about the cyber security.

In our study we focused on the human element and how we can increase knowledge and improve performance, so that the users of critical equipment do not cause infection of malware or do not make bad decisions based on wrong data. We definitely do not want our crews to allow physical access to unauthorized persons, hand over sensitive data or cause data breaches.

The maritime industry is already familiar with learning-by-mistakes, as history shows maritime accidents have resulted in new international regulations, some cyber security cases could also be brought up during the training or familiarization, however one chooses to call it. The seafarers shall be alert and not by their own action cause cyber-attacks or hand out sensitive data or allow access to unauthorized persons with devious intentions. They shall understand consequences. This does not only protect them in their working environment and their employers, but also their personal privacy.

16 Works cited

Agence nationale de la sécurité des systèmes d'information. 2016. *Best practices for cyber security on-board ships.* [Online] https://www.ssi.gouv.fr/uploads/2017/06/best-practices-for-cyber-security-on-board-ships_anssi.pdf (retrieved 11.11.2020)

Ahokas, J., Kiiski, T. 2017. *Cyber security in Ports*. University of Turku: Hazard Project.

BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF & IUMI (version 2.0). 2017. "*The Guidelines on Cyber Security On-board Ships*".

Daum, O. 2019. Cyber Security In The Maritime Sector. *Journal of Maritime Law & Commerce*. 2019, 50(1). p1-19

DNV GL. 2020. ISM cyber security is coming soon – check your preparedness. [Online] https://www.dnvgl.com/news/ism-cyber-security-is-coming-soon-check-your-preparedness-186252?utm_campaign=MA_20Q4_TRN_No%2020_EXT_ISM%20cyber%20security%20is%20coming%20soon%20%C3%A2%C2%80%C2%93%20check%20your%20preparedness&utm_medium=email&utm_source=Eloqua (retrieved 8.10.20)

Drougkas, Dr. A, Sarri, A., Kyranoudi, P., Zisi, A. (2019). *"Port Cybersecurity – Good practises for cybersecurity in the maritime sector".* European Union Agency for Cybersecurity (ENISA)

European Maritime Safety Association. 2019. Maritime Cyber security Table Top Exercise. Presentation by EMSA, 6.3.2019

European Union. 2016. Regulation (EU) 2016/679 of the European parliament and of the council of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (retrieved 11.11.2020)

European Union. 2017. Port Security Awareness – Handbook. [Online] https://www.traficom.fi/sites/default/files/media/file/Handbook_of_port_security_awarness.pdf (retrieved 11.11.2020)

Finnish Shispowners' Association. 2020. Member companies and ships. [Online] https://shipowners.fi/wp-content/uploads/2021/01/Ja%CC%88senalukset-2020.pdf (retrieved 31.5.2021)

Finnish Transport Safety Agency. 2018. Statistics on International Shipping. Lappeenranta: Finnish Transport Safety Agency. https://julkaisut.vayla.fi/pdf8/lti_2018-04_ulkomaan_meriliikennetilasto_2017_web.pdf

Fitton, O., Prince, D., Germond, B. & Lacy, M. 2015. The future of maritime cyber security. Lancaster University.

Gard. 2017. Cyber Security – managing the threat. [Online] http://www.gard.no/Content/21112216/Cyber Security (retrieved 1.10.2020)

Gillham, B. 2000a. *Case Study Research Methods*. Bloomsbury Publishing Plc, 2000

Gillham, B. 2007. *Developing a Questionnaire*. London: Continuum International Publishing Group

Gillham, B. 2000b. *The Research Interview*. London: Continuum International Publishing Group

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A. 2018. Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, p345-358.

Hadlington, L. 2017. Human factors in cyber security; examining the link between Internet addiction, impulsivity, attitudes towards cyber security, and risky cyber security behaviours. Heliyon 3 (2017). [Online] http://dx.doi.org/10.1016/j.heliyon.2017.e003462405-8440/ (retrieved 25.10.2020)

Hadlington, L. 2018. Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. *International Journal of Cyber Crimonology*. 2018, 12(1), p.269-281.

Hadnagy, C. 2014. *Unmasking the Social Engineer: The Human Element of Security*. Indianapolis, Indiana: John Wiley & Sons, Inc.

Henny, C. 2018. Presentation, Brussels 18.09.2018

Hopcraft, R., Martin, K. M. 2018. Effective maritime cyber security regulation - the case for a cyber code. *Journal of the Indian Ocean Region*, 14 (3), p354-366

International Chamber of Shipping. 2016. *ICS Bridge Procedures Guide* (5). London, United Kingdom: Marisec Publications.

International Chamber of Shipping. 2019. *Review of maritime transport*. United Nations Conference on Trade and Development (UNCTAD)

International Labour Organization. 2006. Maritime Labour Convention, 2006, as amended. [Online] https://www.ilo.org/global/standards/maritime-labour-convention/lang--en/index.htm (retrieved 5.11.2020)

International Maritime Organization. [Online] International Convention for the Safety of Life at Sea (SOLAS) [Online] https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx (retrieved 23.1.2021)

International Maritime Organization. 2009. Resolution MSC.282(86). Adoption of Amendments to the International Convention for the Safety of Life at Sea, 1974, as amended. [Online] http://www.imo.org/en/KnowledgeCentre/IndexofIMOResolutions/Maritime-Safety-Committee-%28MSC%29/Documents/MSC.282%2886%29.pdf (retrieved 10.10.20)

International Maritime Organization. 2011. Standards of Training, Certification and Watchkeeping. United Kingdom: International Maritime Organization

International Maritime Organization. 2017. “Guidelines on maritime cyber risk management” & “Maritime Cyber Risk Management in Safety Management Systems” http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/cyber-security.aspx

International Maritime Organization. 2017. ResolutionMSC.428(98). Maritime Cyber Risk Management in Safety Management Systems. [Online] http://www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution%20MSC.428(98)%20-%20Maritime%20Cyber%20Risk%20Management%20in%20Safety%20Management%20Systems.pdf (retrieved 8.10.2020)

International Maritime Organization. Maritime cyber risk. [Online] https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx (retrieved 31.5.2021)

International Maritime Organization. Maritime Security and Piracy. [Online] https://www.imo.org/en/OurWork/Security/Pages/Default.aspx (retrieved 31.5.2021)

International Maritime Organization. Multilingual glossary on cyberterms. [Online] http://www.gard.no/Content/21112214/CYBERTERM_Imo.pdf (retrieved 1.10.2020)

International Maritime Organization. SOLAS XI-2 and the ISPS Code. [Online] http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx (retrieved 4.10.2020)

International Maritime Orgnaization. 2007. ResolutionMSC.252(83). Adoption of the Revised Performance Standard for Integrated Navigation Systems. London. [Online] https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.252(83).pdf (retrieved 31.5.2021)

International Maritime Orgnanization. 2014. International Safety Management Code (4). London, United Kingdom: International Maritime Organization

Jaf, S., Ghafir, I., Prenosil, V., Saleem, J., Hammoudeh, M., Faour, H., Jabbar, S. & Baker, T. 2018. Security threats to critical infrastructure: the human factor. *Journal of Supercomputing*, 74(10), p.4986-5002.

Klossner, J. [online] http://www.jklossner.com/kopkf22ta931lmnlmaj3h48vplhotb (retrieved 20.3.2021)

Kohn, A. 2014. Brain Science: Overcoming the Forgetting Curve. [Online]

https://learningsolutionsmag.com/articles/1400/brain-science-overcoming-the-forgetting-curve (retrieved 7.10.2020)

Kohn, A. 2014. Brain Science: The Forgetting Curve – the Dirty Secret of Corporate Training. [Online] https://learningsolutionsmag.com/articles/1379/brain-science-the-forgetting-curvethe-dirty-secret-of-corporate-training (retrieved 5.10.2020)

Kusi. B. 2015. *Port Security – Threats and Vulnerabilities*. Thesis for Bachelor of Security Management. Laurea University of Applies sciences, Leppävaara, Finland

Li, L., Xu, L., He, W., Chen, Y., Chen, H. 2016. Cyber Security Awareness and Its Impact on Employee's Behavior. 10th International Conference on Research and Practical Issues of Enterprise Information Systems (CONFENIS), 2016, p.103-111. [Online] https://hal.inria.fr/hal-01630550/document (retrieved 25.10.2020)

Lloyd's Register. 2016. *Cyber-enabled ships*. [Online] https://info.lr.org/l/12702/2016-02-19/2q46sl/12702/138839/lr_guidance_note_cyber_enabled_ships_february_2016__3_.ppd (retrieved 20.3.2021)

National Cyber Security Centre. Instructions and guides – Tips for keeping your information safe. [Online]
https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet.html
https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides (retrieved 20.3.2021)

National Cyber Security Center. 2016. *Common cyber attacks: reducing the impact*

McDonough, B. R. 2019. *Cyber Smart: Five habits to protect your family, money, and identity from cyber criminals*. Indianapolis: JohnWiley & Sons, Inc.

McNicholas, M. 2007. *Maritime Security: An introduction*. Burlington, Massachusetts: Butterworth-Heinemann publications.

Mraković, I. and Vojinović, R. 2019. Maritime Cyber Security Analysis – How to Reduce Threats? *Transactions on Maritime Science*. Split, Croatia, 8(1), p. 132 - 139

Ording, K., 2019. *Ethical Hacking*. DNV GL [Online]
https://www.dnvgl.com/feature/ethical-hacking.html (retrieved 11.11.2020)

Pajunen, N. 2017. *Overview of Maritime Cyber security*. Thesis for Bachelor of Marine Technology. South-Eastern Finland University of Applied Sciences, Kotka, Finland.

Ringbom, H. 2008. *The EU Maritime Safety Policy and International Law*. Leiden: Koninkilijke Brill NV.

Roediger, H. L. III & Brown, P. C. 2020. The Importance of Testing as a Learning Strategy. *Education Digest*, 85(3), p.11-16.

Rossbach, L. 2017. EMSA, Workshop "Cyber-Attack Prevention" 13 - 14 December 2017 – EMSA, Lisbon Portugal.

Rothblum, A.R. 2000. *Human error and marine safety*. [Online] http://www.dtic.mil/docs/citations/ADA458863 (retrieved 8.10.20)

Sales, N. A. 2013. Regulating Cyber-Security. *Northwestern University Law Review*, 107(4), p.1503-1568.

Salmon, A., Levesque, L. & McLafferty, M. 2017. *Applied Network Security*. Birmingham: Packt Publishing Ltd.

Salzman, D. 2020. *Are Cruise Ships Safe?* [Online] https://www.cruisecritic.com/articles.cfm?ID=241 (retrieved 28.10.2020)

Schuster, S.& Polemi, N. 2019. Workshop on cyber security in maritime sector. Presentation, Brussels 4.9.2019

Silgado, D. M. 2018. *Cyber-attacks; a digital threat reality affecting the maritime industry*. Thesis for Master of Science in Maritime Affairs. World Maritime University, Malmö, Sweden.

Statistics Finland. 2021. Merchant Fleet [Online]. https://www.stat.fi/til/klaiv/index_en.html (retrieved 18.10.2020, 31.5.2021)

Statistics Finland. 2020. Gross tonnage of the regular Finnish merchant fleet increased in 2019. [Online]. http://www.stat.fi/til/klaiv/2019/klaiv_2019_2020-02-26_tie_001_en.html (retrieved 18.10.2020)

Svilicic, B., Brčić, D., Žuškin, S., Kalebić, D. 2019a. Raising Awareness on Cyber Security of ECDIS. *TransNav: International Journal on Marine Navigation & Safety of Sea Transportation,* 13(1), p.231-236

Svilicic, B., Kamahara, J., Rooks, M., Yano, Y. 2019b. Maritime Cyber Risk Management: An Experimental Ship Assessment. *Journal of Navigation*, 72(5), p.1108-1120

Svilicic, B., Rudan, I., Francic, V., Doricic, M. 2019c. Shipboard ECDIS Cyber Security: Third-Party Component Threats. *Scientific Journal of Maritime Research*. 2019, 33(2), p. 176-180

Tam, K., Jones, K. 2019a. Maritime cyber security policy: the scope and impact of evolving technology on international shipping. *WMU Journal of Cyber Policy*. 2018, 3(2), 147-164

Tam, K., Jones K. 2019b. MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*. 2019, 18, p. 129-163.

Ulsch, M. N. 2014. *Cyber Threat! How to Manage the Growing Risk of Cyber Attacks*. Hoboken, New Jersey: John Wiley & Sons, Inc.

United States Coast Guard. 1995. *Human factors of Electronic Chart Display and Information Systems*. Washington, D.D.: Department of Transportation.

Voeller, J. G. (ed.) 2014. *Cyber Security.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Walliman, N. 2010. *Research Methods: The Basics*. Taylor & Francis: e-Library.

Wilson, A. M. & Likens, G. E. 2015. *Content Volatility of Scientific Topics in Wikipedia: A Cautionary Tale*. 10 (8), p.1-5.

Wikipedia. Cyber Security. [Online] <https://en.wikipedia.org/wiki/Computer_security> (retrieved 4.10.2020)

Appendix 1

Cyber security in Finnish maritime domain

Study on cyber security awareness in Finnish ports and shipping companies

Thesis questionnaire on cyber security (Shipping companies)

Briefing for the interviewees:

The authors of the thesis with a title “Cyber security in Finnish maritime domain” are Stella Wallenius and Henri Wallenius. We study at Novia University of Applied Sciences; the name of the degree program is “Autonomous Maritime Operations”. One of the topics of our thesis work is to study cyber-security awareness in Finnish shipping companies (also ports). This part of the study is done by qualitative research.

We want to thank you for this opportunity to use your expertise and experience in our thesis work. We have selected five Finnish shipping companies to give their views on this topic. All interviewees are company security officers (CSO). This position (CSO) is mandatory duty according to the IMO ISPS code and other relevant regulations. In our view the holders of this position are the most suitable persons to answer our questions, since in your role is the overall safe and secure operations.

All discussions and answers will be handled with confidence. We will not report or name individual shipping companies or name of the interviewees, the results of these interviews will remain fully anonymous. We will report only the number of interviews and the findings will remain anonymous throughout the thesis report. All interviews are done personally by bilateral discussions.

Questions for the interviewees:

1. In your understanding what is a cyber security and cyber security risk? (Explain in your own words what a cyber-security risk is)

2. What are generally the most important security gaps in you view? (Give your general view on this, not necessarily related to your own company, but from a wider perspective in maritime context)

3. In your opinion and considering your own organization, where is room for improving cyber security measures? (Now focusing to your own company, evaluating the weak points)

4. Has your company encountered a cyber-security attack, or some other intentionally caused problems related to ICT issues?

   Malware (any software intentionally designed to cause damage to a computer, server, client, or computer network)

   Ransomware (type of malware from crypto virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid)

   Phishing (fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details or other sensitive details, by impersonating oneself as a trustworthy entity in a digital communication)

   Spam (use of messaging systems to send an unsolicited message (spam) to large numbers of recipients for the purpose of commercial advertising, for the purpose of non-commercial proselytizing, or for any prohibited purpose (especially the fraudulent purpose of phishing)

   Social engineering (social engineering is the psychological manipulation of people into performing actions or divulging confidential information)

   Other

5. Do you recognize who is in charge of your company’s ICT and cyber-security?

   Yes / No / Other comments

6. Is your company's ICT functionality outsourced?

   Yes / No / Other comments

7. Has your company implemented cyber security as a part of safety management system

   Yes / No / Other comments

8. Has your company made a risk evaluation and analysis on cyber-security risks?

Yes / No / Idk / Other comments

9. How high do you estimate the likelihood that your own business activity will encounter a cyber-security incident?

   Not likely / very likely scale 1-5

   Other comments

10. In your honest opinion what is the level of awareness of your own personnel on cyber-security?

    Low level of awareness / High level of awareness

    Other comments

11. Do you organize cyber-security related drills and exercises?

    No / Yes

    Other comments

12. Internet access from ships. Is there recreational internet. Is there rules for the usage?

    No / Yes

    Other comments

13. Any other perspectives you want to bring up?

Cyber security policy for ships in Company X

Every shipboard employee in the company shall have read this document prior to boarding. Be prepared to discuss or answer questions related to these issues during the familiarization on-board.

COMPUTERS on the bridge and in the engine room

- Shall not be used for browsing the internet or other recreational use. Only task specific defined applications shall be used on these computers.

OTHER COMPUTERS can be freely used. However:

- NEVER plug in your private mobile phone
- NEVER plug in other mobile devices (USB-memory stick for instance) unless its content and source are 100% known
- NEVER connect them to your own mobile network

There have been cases where a virus has spread to the computers and even further to other systems and equipment on-board via internal connectivity. Disturbance in route planning / ECDIS or engine control systems may have severe consequences. At minimum they cause technical problems, delays and costly need for service work. Infected devices must be cleaned.

E-MAIL is a very common channel for malicious use. Regardless of private or work e-mail, you shall

- BE CAUTIOUS when opening attachments. If you are not expecting something specific or the sender or message include anything suspicious, do not open it
- BE CAUTIOUS when clicking on links in e-mails. Only do so when you know the sender and even then, pay close attention to the sender's e-mail address. Example: an address with NORPELY@vero.com may look like from the Finnish tax office. But a closer look reveals that is not the case.

Malware can spread to the computer via e-mails (attachments or links). They may seem legitimate, but when looking closely, there is something wrong with it.

SERVICE WORK to shipboard computers and systems

- IS ALWAYS ordered by the office and the authentication of the service personnel boarding shall ALWAYS be verified.

We must have complete control of what is being done and by whom to our computers, other equipment, systems and networks and if new faces appear, remember to check for their ID-card and compare with what has been ordered.

UPDATING ECDIS and other systems in use on-board

- SHALL ONLY BE DONE by verified persons or through verified means. If an update is provided on a USB-device, you must confirm that it is legitimate. If it is done remotely, you must confirm the service provider before granting remote access.

ANTIVIRUS AND FIREWALLS shall always be updated. We aim to arrange those automatically from the office but

- IF THERE IS A WARNING saying that the antivirus- or other protection is outdated, you must inform the office
- NEVER install or update anything yourselves.

PERSONAL DATA can only be accessed by managers and office. The European General Data Protection Regulation requires that

- PERSONAL DATA can only be handled by those who need it in their work
- PERSONAL DATA must be deleted when no longer needed

Our crew management system fulfils these rules, including back-up. Take care of your own documents and when handling others', be careful and do not take copies if not needed! When using company e-mail, remember to regularly (at minimum every 6 months) to clean both the inbox but also the sent-folder from personal data.

BUSINESS-SENSITIVE DATA such as financial information or contracts

- SHALL ONLY BE KEPT in appropriate folders. Do not print or take copies or store them electronically in other locations than agreed.

You can never be too suspicious. If something seems strange, **use some extra minutes to confirm the situation** (a removable device, attachment in an email or a link with an update to your computer system). This is much easier than cleaning up the mess afterwards. Attacks can be intentional or random. A random attack is aimed at several networks and where it finds a security gap, it does its harmful acts. We will cooperate together not to be that security gap!

THANK YOU AND STAY CYBER SAFE OUT THERE!

MALWARE

FIREWALL

PASSWORD

ANTIVIRUS

BUG

OUTDATED

SENSITIVE DATA

PHISHING

AUTHENTICATION

SCAM

VIRUS

SPAM

GDPR

CYBER ATTACK

ATTACHMENT

UPDATED

CYBER SECURITY

Appendix 3

Addressing cyber security during shipboard familiarization in Company X

We have delivered the company policy related to cyber security in advance to all new employees. In order to refresh their memory and to understand the importance, here are a few questions and comments to address during the familiarization:

- Were you familiar with the cyber security -issues in our document?
- What did you think? Anything more/less you would like to point out?
- Have you experienced cyber security incidents before (at work or in private life)?
- What do you think are the biggest risks on our ship (what could be most likely to happen)?

Remember to show the computers and which one(s) are meant for private use. Remind the new employee about not sharing mobile internet connection and not plugging in their own devices to ANY computers on-board.

IN ADDITION, if the new employee will be handling personal data:

- Are you familiar with handling of personal data? What does it mean in practice?
- What kind of processes are you used to when handling personal data, especially in email? We could use some good practices!