Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

KONSTA MAUNULA

Human role in maritime cyber security onboard the vessel

NMM18SR
2022

Author
Maunula Konsta

Type of Publication
Bachelor's thesis

Date
April 2022

Number of pages
29

Language of publication:
English

Title of publication
Human role in maritime cyber security onboard the vessel

Degree Programme
Sea Captain

Abstract

The purpose of this thesis is to do qualitative research on the maritime cyber security sector threats and find out how the cyber breaches are performed and how they impact vessel operations. I also research ways how to prevent attacks from occurring. To limit the topic, I took the perspective of the ship officer in this thesis. I focus on finding out how the ship crew can prevent possible cyber attacks and what are the best practices in daily ship operations.

The hypothesis for thesis is that in general, cyber security exploits need a human error to be possible. Nowadays, the risk of cyber security breaches are increasing due to technologicalization in vessels operations.

There are publications and research done about cyber security in shipping but, I felt that there is a need for compact summary and practical approach to the situation in maritime cyber sector. Therefore, my approach is firstly, to study all latest information about the topic and from the latest and relevant breaches. Secondly, I then explain common cyber security risks in the vessels working environment. Thirdly, I examine the common attacks with examples, how such attacks are performed and whether they can they be prevented by the crew. Furthermore, I go through the regulations and insurances covering maritime cyber security. Finally, in the last chapter I present my conclusions and findings and provide basis for future research.

The results are alarming due to high number of available exploits with limited equipment needed. Many attacks can be prevented by good cyber hygiene by crew but there were available exploits that could interfere with safe navigation of vessel. Officers' education and experience are tested in case if attack reach operational technology systems specially during sea voyage. My research shows that the level of education of crew on cyber crime threats is surprisingly low. There is not enough obligatory training. This Merits attention and should be better addressed. Investments in education of crew about cyber attacks should be high priority for every shipping company, because it has been shown to have significant impact of reducing the amount of successful cyber exploits.

Keywords
Cybersecurity, Human factor, GNSS

AIS	Automatic Identification System
Backdoor	Mechanisms used to access undocumented features or interfaces not intended for end users
Bandwidth	Maximum amount of data transmitted over an internet connection in given amount time
Brute force	Hacking method that uses trial and error to crack passwords
COLREG	Convention on the International Regulations for Preventing Collisions at Sea
Domain	Refers to group of users, workstation, devices, and database servers that share different types of data with network resources
GMDSS	Global Maritime Distress and Safety System
SOLAS	Safety of Life at Sea
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IMO	International Maritime Organization
ISM	International Safety Management
ISPS	International Ship and Port Facility Security Code
IT	Information Technology
OOW	Officer of the Watch
OT	Operational Technology
SMS	Safety Management System
SSP	Ship Security Plan
STCW	Standards of Training, Certification and Watchkeeping for Seafarers
URL	Uniform Resource Locators
VPN	Virtual Private Network
Wi-Fi	Is all short-range communications that use some type of electromagnetic spectrum to send and/ or receive information ismout wires.

CONTENTS

1 INTRODUCTION

The purpose of the thesis is to take broad look at the maritime cyber security sector and provide ship officers and maritime organizations tools to defend against cyber threats. I chose the topic because nowadays, on ships, cyber security has become an important part of the security aspect and a risk management on vessels and will only continue to increase as we can see later in the study. Cyber attacks have been on the rise recently and shipping companies have noticed this. Since February 2020 there has been 400% increase in cyber breaches at maritime industry. (Security Magazine, 2020). Understanding how the attacks are performed and how they impact the operations of the vessel gives tools to crew to prevent most of the attacks.

Research about the topic have been done earlier, but I felt that there is a need for up to date material for maritime students, however crew can utilize it onboard also, to get knowledge about cyber security. It was not the intention of this study to purely look only technical aspect of the exploits, but to give well rounded overview of the attacks and info to officer how to prevent them.

First, I show the common exploits in cyber security, how they are performed and their impact on the operation of the vessel. Secondly in the research I point out the biggest weaknesses in vessel Operational Technology and Information Technology systems and how they can be exploited. At last, we go through ways to prevent the attacks and the legislations in cyber security, and I present my conclusions.

According to my experience cyber security onboard depends too much on the crew's self-study and the unproper practices on cyber hygiene often leads to incidents. Usually there is short cyber security course for the crew to complete onboard, but this gives only introduction to cyber security which is not enough.

Technology has enabled shipping to become much more cost efficient, but it has also created new risks. Given the impact of these technology robust cyber security and frameworks are needed to maintain seaworthiness. In modern times it is possible to infect the system with a bug or virus, which can lead to a crash of the entire system or lead to malicious actor gaining control of the vessel operating system, this also includes vessels propulsion systems.

Study conducted by (IBM, 2020) shows that 95% from cyber security breaches were caused by human error. From one hundred cyber security violations ninety-five would be removed if the human factor were to be removed. The first target of an attack is not usually company network, it is people. If the crew does not fall short in the basics of cyber security the attack usually fails.

2 CYBER SECURITY AND COMMON SECURITY THREATS

Cyber security should protect critical data and systems from cyber attacks. In modern times working environment it is easy to think that the risks are well known which is not the case. According to CSO alliance more than 1,000 ships have been hacked in the last five years. (CSO Alliance, 2021). Malicious actors are all time finding new ways to jeopardize company's operations. Even for well-trained professionals, it is hard to keep up with cyber threats. Essential part of cyber security is understanding that everything in today's world is connected through internet. Every system needs to be protected individually; it is not enough to protect one alone. If you infect one software or program in the network, it can quickly spread through the whole company network. You do not need to use much imagination to understand that if cyber criminal is able to take control of vessel, what damage it could cause.

Attacks on operational technology has become increasingly more threating every day due to reliance on third party services and Global Navigation Satellite systems. Outdated OT systems pose a substantial risk to cyber security as malicious actors are constantly finding new ways to jeopardize operations on vessel and situation is not expected to improve soon. The number of cyber threats in maritime sector is so alarming that it is hard for even well-trained professionals to keep up with the sector. International Maritime Organization has also recognized in their meeting sixteen. June 2017 to urgent need to raise awareness on cyber threats and vulnerabilities to support safe and secure shipping. Everyone with a laptop and the needed skills can cause large amount of damage in cyber sector. To understand how to protect against these threats we need to know how cyber attacks are created. (IMO, 2017).

2.1 Motivations behind the cyber crimes

Attackers usually have some goal in mind what they want to achieve with the attack. Goals include things like:

- Business financial data
- Email addresses and login credentials
- Intellectual property, like trade secrets or product designs
- IT infrastructure access
- Sensitive personal data
- Access to vessel operations

Malicious actors are often quite different from one another, what the goal behind the attack is. In addition, cyber attackers can also include cyber warfare or cyberterrorism, like hacktivists. (IBM, 2022.)

2.2 Spoofing

Spoofing is done by sending identical signal that is strong enough to block out the correct signal. Once the incorrect signal of satellite is in place, malicious actor can send signals to influence on vessel movement. (Louie, 2019.) According to Roi Mit (2019) chief marketing officer at Israel-based cyber security firm Regulus Cyber: *"Software-defined radios (SDRs) which are used to spoof signal are cheaply available online, and with the right software can be used to mimic satellite signals to transmit fake ones"*

Maritime industry is starting to wake up to these threats. In study done by C4ADS (2019) 9883 suspected spoofing instances in ten separate locations that affected 1311 civilian vessel navigation systems since February 2016.

Officer Of the Watch should be ready to respond to these threats and always verify the signal from other sources for the possible spoofing events of GNSS systems. Continuing increase in spoofing accidents and the easy to obtain spoofing devices online make it dangerous and can have severe consequences to safety of navigation.

Lack of encryption of navigation data and security measures make GNSS not up to date to respond to these security threats. Due to these threats it is important for the navigator to not rely on Electronic Chart Display and Information System (ECDIS) data only.

2.3 Malware and Ransomware

Most well-known malware attack in maritime industry is Maersk case. In 2016 there was well known vulnerability in Microsoft system. While it was patched shortly, not all organizations updated it immediately. It is important to understand that Maersk was not even the target in the attack. This shows how quickly malwares can spread throughout organizations. Maersk was saved by the fact they had one offline domain. Whit this domain they could restore IT systems, otherwise damages would have been even more devastating. (Louie Chris, 2017.)

Malware and ransomware are often remarkably similar attacks. Malware is general term for any program that purpose is to damage, disrupt or hack a device. Ransomware however is program that is designed to block access to device, usually it is difficult to remove. Ransomware also includes ransom that needs to be paid before access to device will be restored. (Kate Veale, 2022.)

Malwares are often spread by file sharing, downloading, free software, email attachments, using compromised portable storage devices and infected websites. Malwares can affect device in numerous ways including slow device performance, loss of data, corrupted program and files or completely shutting down device. (Kate Veale, 2022.)

Ransomware locks you out of your systems and demands something for release. Most advanced ransomware attacks have been able to encrypt files and you need the key to open it. Ransomwares most common way of distribution is email phishing. (Kate Veale, 2022.)

Best and most effective way to protect your company against malware and ransomware attacks are quite simple and easy to do. Keeping software up to date is key in protecting against malware. Having your staff educated enough to spot phishing messages on email or from text messages to mobile phone is also essential. Even if the message is sent from trusted source, does not mean it cannot have virus behind hyperlink. Knowing where you can connect your own device and where it is completely prohibited is an important part of the company's safety. Identifying risk points on company and vessels systems is an efficient way to protect against cyber crimes. (Kordia, 2017.)

2.4 Social engineering and Phishing

Lord (2018) has defined social engineering in this way; "*Social engineering is defined in cybersecurity as a "non-technical strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices*"

Phishing is a type of social engineering, it occurs when an attacker, acts as a trusted entity, dupes a victim into opening an email or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. (Imperva, 2021.)

Proofpoint's (2021) report shows 99% of cyber attacks use social engineering techniques as a part of the attack to trick crew members into installing malware. This also includes phishing with text and emails which is also a part of social engineering.

Social engineering is often recognized the most effective way for malicious actor to get access in company´s operations, people are often the weak link. Humans can be very easily tricked and manipulated to break security practices. Without good knowledge about social engineering techniques success rate on the attack according to Cyber edge (2017) was 79%.

Social engineering and phishing can be very targeted to one specific company worker with good background information gather or it can be just phishing email messages to every company worker to find a weak link.

Social engineering is becoming difficult for organizations to defend. Traditional social engineering include phone call or text message usually involves urgency. There is the straightforward way to defend it, following company's procedures and operating with zero trust, but that has been shown to be easier said than done. It is important to be suspicious during interaction and not to share any critical information.

Crew`s education about the social engineering is vital for organization safety. Every crew member should be educated enough to know how to use spam filters, to check if the email really came from stated recipient, think before providing sensitive information and to pay attention to uniform resource locator. URLs are in simple words web addresses used to locate web pages on internet. (Scarpati & Burke, 2021.)

2.5 Distributed denial of service (DDoS)

Distributed denial of service is a cyber attack on a specific server or network intending to disrupt normal operation. It floats the target with constant traffic which overwhelms the systems and causes denial for service for legitimate traffic. If the attack is coming from only one source, usually the server can point out the attack and close the connection, that is called only denial of service attack. If one computer communicates with many other computers to coordinate attack at the same server at the same time, this causes server to deal with attack from multiple sources. It leads server to be too occupied and the legitimate computers cannot access the server, or they will be slow on loading. Most of the time DDoS attacker gets the other computers to attack the server at the same time with previously mentioned malware attack to gain access on enough computing power (Cloudflare, 2022.)

Cisco (2018) report estimates that amount of DDoS attacks will increase from 2021 ten million up to fifteen million in 2023. To put this into perspective it means nearly every business has faced one after 2023.

DDoS is still mostly unknown attack in maritime industry and specially towards vessels. With increasing amount of OT technology and automation it is evident that DDoS attacks will increase, and we have not yet seen how effective they can be towards vessel servers.

Effective way of defending against DDoS attacks is increasing bandwidth, this has limit though and the costs of the increasing bandwidth are high. This however increase the threshold for the DDoS attack because attacker needs more computing power to jam the network. Up to date software, hardware and firewall are key in defending against also in DDoS attacks.

DDoS attacks can be especially malicious against OT systems, due to many of the OT systems are designed to be offline but increase need of connection to shore has placed many of the old OT systems to online. For example, case where botnet is installed by unscanned USB stick to vessels system. Botnets infect computerized hosts and broadcast on open ports to discover additional hosts to infect on rapid pace. Malicious actor can put the botnet on timer, and it goes unnoticed. When systems are online the hacker can get control of thrusters. (Cloudflare, 2022.)

3 CYBER SECURITY ONBOARD

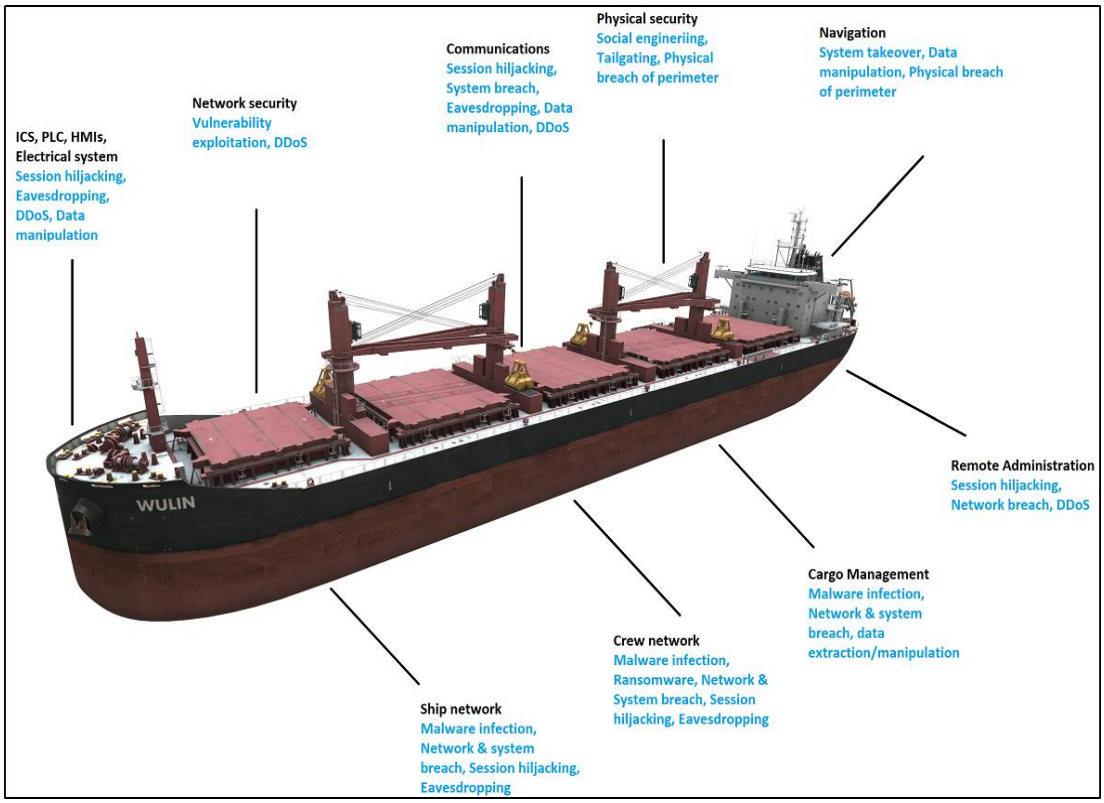

Figure 1. Common cyber security threats (source: www.huoltovarmuuskeskus.fi)

To put it simply there are two types of attacks vessel can encounter: untargeted or targeted attacks. It was estimated for cyber attack to took 279 days to become incident. Untargeted attacks can be as dangerous for the vessel's security for example Maersk in 2017 cyber breach was not the intended target and the cost for Maersk is estimated to be around 200-300 million us dollars. From the figure it is easy to understand that there are many ways the attacker can get access of the vessel’s operations and some of them are not even known yet. (IMO, 2017.)

3.1 Where the attacks are coming from

Vessels in 2000-centry are build lots of technology in hand. Vessel operations are many times very dependent of extremely advanced technological solutions.

Advancements in technology and decreasing crew sizes have made life onboard challenging. Most of the time vessels have own servers, Wi-Fis are common onboard which can pose high risk. So, it is coming clear to maritime industry that technology is advancing in vessels, but there are no IT people at vessels. Often ship's crew members are on their own with the IT problems. It is quite common onboard that electrician is solving software-based problems, without any education for the job. (Elgan Mike, 2021.)

Cyber attack can occur from outside threat or inside threat. Inside threats include:

- Employees careless security policies and procedures
- Disgruntled current or former employees
- Business partners, clients, contractor, or suppliers

Outside threats include:

- Organized criminals or criminal groups
- Professional hackers, like state sponsored actors
- Amateur hackers or hacktivist
- Governments

It is important to be prepared for these risks and have good cybersecurity system applied onboard which effectively reduce the risk of infection. (IBM, 2022.)

3.2 GNSS

Global Navigation Satellite System is integral part of today’s OOW navigation tool kit. Even though use of radar and sight still stated in COLREG to be primary decision-making tool in navigation. GNSS should be used as navigation aid to help navigator to make decisions. But reliance in GNSS systems in today’s navigation has become imminent, this poses substantial risk for the vessels navigation. Spoofing events of GNSS are increasing in maritime industry and the need for robust cyber security frameworks are needed. (Novatel, 2015.)

3.2.1 GPS

Today's navigation relies on Global Positioning System to give navigation officer the position of the vessel through ECDIS monitor. GPS consists of these systems:

- Satellites
- Ground stations
- Receivers

With these three systems navigators can get positions of vessel, but the data is open-source and possible to interfere. Vessels equipped with ECDIS as main navigation charting system without up-to-date paper charts rely on correct GPS signal, if the GPS signal is not correct, ship cannot operate safely. (Lo Chirs, 2019.)

Malicious actor can spoof or jam the GPS signal. GPS spoofing allows hacker to interfere with vessels GPS signal and to misdirect vehicle out of her course. GPS spoofing is done by overpowering the correct signal with false satellite signal. This works because of the navigation systems are designed to use strongest GPS signal most of the time. (Duncan Parnell, 2020.)

GPS jamming is done by sending radio signals on same frequency as the GPS device to overpower correct signal making it unable to determine its position. Jamming device requires to be close to the GPS tracker to work. Jamming is much easier to detect because system will be unable to produce vessels position. (Duncan Parnell, 2020.)

Study done by University of Texas shows how 65m yacht was successfully hacked and given fake position. This was made with GPS spoofing device which broadcasted faint civil GPS signal. This overpowered the correct GPS signal and they gained control of the ship's navigation. After control was gained, they slowly changed course with minimal manoeuvres, about few degrees off its original course. Ship crew found out by off track alarm that ship is sailing away from its intended course, and they made alterations to keep vessel on its track. What happened in fact was that the ship sailed with each manoeuvre more away from its intended course. After many fore mentioned manoeuvres researchers had successfully tricked ship to parallel course. (Todd Humphreys, 2013.)

Bhat (2013) director of the centre of Transportation Research at UT Austin believes that *"Experiment highlights the vulnerability of the transportation sector to such attacks"*.

3.2.2 AIS

On this day Automatic Identification System have become valuable tool in navigational officer's kit. It gives much information about surroundings and is easy to use. That is why it has become so popular, but false picture about surroundings could mislead OOW in navigation. Threats to AIS are categorized by (Androjna et al., 2021) to these three categories: Spoofing, hijacking, and availability disruption, based on software or radio frequency. AIS messages are neither encrypted nor authenticated which make them vulnerable to exploits. AIS vulnerabilities come from open-source system without encryption that transmits in VHF channels therefore putting it risk on data manipulation.

In 2019 UK-flagged product tanker fell victim of AIS spoofing attack. It altered it course into Iranian waters and her cargo and crew were captured. This caused vessel over 2-month laytime and most of the crew were held captured. According to (Boyle, 2019) Lloyd's List Intelligence: "there are some strange AIS messages which indicate the GPS used in the AIS message have been spoofed". Crew reported that they had to repair the course which is usually what happens in spoofing. (Bockmann, 2019.)

Bursting out an overload of incorrect VHF signals to AIS can mislead OOW hazardous situations. False signals wish are displayed on ECDIS and RADAR screen from AIS gives wrong indication about the current situation and can lead to accidents if the OOW is not ready to response to the threat in hand. Experienced navigator can change the radar picture to "raw" and use visual look out to avoid the danger and proceed safe passage. (Androjna et al., 2021.)

3.3 Satcom

Satellite communication systems in maritime are used to provide communication solutions to maritime industry. Satcom importance in today's vessels operations have become quite minimal in most cases, but for example IMMARSAT is still part of Global Maritime Distress and Safety System regulations under SOLAS convention and is often solution vessels that operate in A3 areas. Satcom vulnerabilities come from:

- Hardcoded credentials
- Undocumented protocols
- Insecure protocols
- Weak/poor password reset procedures
- Backdoors

Vessel network in some cases can be accessed through satcom terminal if good segregation of vessel networks has not been done. Without good segregation of vessel network, it is possible to gain access to vessel OT systems from using Satcom as a tool. This is accelerated due to location of vessel being available to public in real time. It has been shown that terminals are often poorly designed and accessible from public internet. Satcom is also victim of its public satellite system which has its own weaknesses. Measures against public internet access on Satcom should be taken. (Isaac R & Porche III, 2020, 318)

3.4 Network

Vessels today depend on many third parties on operation of their critical systems and assets. Threats against entirely on IT systems are much easier to identify due to much more evidence about the attacks, but the threats to these systems should not be underestimated.

Secure networks minimize the amount of entry points it has and control the ones that are available. Network layout should be planned beforehand for every new vessel.

Every network should include administering and managing network on dedicated workstations. Servers should provide file sharing, email, and other services to the network. Physical layout of the network should be restricted access area to avoid any not desired individuals to gain access on network. (BIMCO et al., 2021.)

Monitoring data and detecting unauthorized data traffic should be self-evident for every company's IT department. Intrusion detection system or Intrusion protection system should be set in place to get alert in real time of attacks to network. They inspect data going through entry points and reject traffic which does not comply with company security policy. Protection can also be placed by remote access segment like VPN. (BIMCO et al., 2021.)

4 DEFENDING AGAINST CYBER THREATS

Defending against cyber security should be done in multiple layers which includes role of employees, procedures, and technology. These measures should decrease the likely hood of cyber incident and increase probability that a cyber incident is detected. Implementation of cyber security in company risk assessment should be done in vessels systems to determine critical technology for operations and to find out the possible threats. (BIMCO et al., 2021.)

4.1 Cybersecurity Plan

Each vessel must have a cyber security plan. The security plan should contain a reference to cyber risk management procedures found in International Safety Management Code. In International Maritime Organization Resolution MSC.428(98) its stated that Safety Management System should include cyber risk management. Maritime safety committee states that Ship Security Plan should include also cyber security aspect. At least these things should be stated in SSP:

- Procedures related to physical access to areas with IT and OT systems
- A reference to the SMS cyber security procedures.

Company should also consider if there is need for vessel specific IT/OT system based on if ships have unique IT/OT systems. (IMO, 2017, 8-9.)

Effective cyber security plan should also consider safety and security impacts after exploitation. Plan should include what are the best practices crew should use after incident and what is the way of moving forward after the incident. The plan should include effective offline copies of the systems so that they can be restarted from scratch. Systems that that are vital for operation of ship should include backup systems. Offline backups are the most bullet proof method of cyber security because they are not connected to internet and are impossible to hack. Crucial quick access to support in case of cyber incidents should be addressed in plan, crew needs to have all time available connection whit IT department.

4.2 Segregation of Network

One of the most important ways to defend against cyber attacks is segregating networks and OT systems from one another. Depending on the importance of the system stricter safety measures should be applied. In vessels where there is high level of integration, which is often the case in new vessels, high level on layering protection should be applied, to make sure all crucial systems are protected, and the bug cannot spread across vessel systems. (BIMCO et al., 2021.)

Onboard networks should normally include the following: 1. Necessary communication between OT equipment. 2. Configuration and monitoring of OT equipment. 3. Onboard administrative and business tasks including email and sharing business related files or folders. 4. Recreational internet access for crew and/or passengers/visitors. (BIMCO et al., 2021.)

4.3 Password security

Password security is key in vessel cyber security because of brute force techniques hackers use to get access to devices. Malicious actors can get up to 669 million passwords tries per second with newest graphic cards. The hacker can specify brute force attack to use for example no symbol. If malicious actor has idea of what word password might be hacker can use brute force with the word and try all possible number & symbol combinations.

If vessels device password is for example such simple as admin or vessel it is putting cyber security onboard at enormous risk because every hacker tries them first and it is surprising how often they work. The company's ships are looking for trouble in terms of cyber security and many carefully thought-out cyber security practices are wasted because a hacker gets through them in seconds due to laziness in password security.

Crew members onboard have the most responsibility in password security. According to study done by (Security.org Team, 2021) 68% percent of people use same password for different accounts.

Never reuse password or use personal information on password these are simply ways to avoid password cracking. It is essential to randomize your password with at least ten characters including symbols, capital letters and numbers included. It is important because, for example, seven lower case letters and one number in your password can be hacked in less than two hours without any prior knowledge of the password. (Stouffer Clare, 2021)

The login page should not provide any additional information about the password to the user. The login page should not provide this type of information when logging in: the password is incorrect. This should be corrected and formatted that the password or username is incorrect. Giving unnecessary information to a hacker should be avoided because if a hacker finds out the password is correct, half the work is completed and all that needs to be done anymore is to hack your username

Log in attempts should be minimized to 5-10. This significantly reduces chance of brute force success. Using multi-factor authentication has become more popular in companies cyber security and it has been noticed that it greatly increases password security

4.4 Device connecting

It has become common for external companies to connect their devices with ship's equipment, but this is also one significant risk factor in cyber security. Every device that connects to important systems onboard should be scanned for malware. There should be procedures that prevent and restrict use of USB devices including visitors USB devices.

USB sticks that are used for transferring or storing crucial data about vessel operations should not be used anything other than that. Using those USB sticks for transferring movies is not good cyber hygiene and can lead to exploits. it is a simple matter but has led to many accidents and in the worst case gives the malicious actor direct access to the ship's operations

4.5 Training

Cyber security firm NSSGLOBAL shows that 84% crew members claimed that they have received little or no training from their employees about cyber security. (NSSGLOBAL, 2017). Training about cyber risks is not mandatory requirement for crew. This just shows how far maritime sector is at effective cyber risk management. Training has been shown to have great effects in fighting against cyber risks because most of the incidents are happening due to crew members fail do to very basics.

All shipping companies should start providing basic cyber awareness training for crew and employees with designated duties in cyber risk management or have crucial part in vessel operations. These exercises should be designed specifically for those persons inside the company. Basic drills about cyber security should include basic things such as information sharing about company, device connecting, knowing about common cyber attacks and how to deal with them, how to spot phishing from email or texts and other means of good cyber hygiene.

BIMCO and the International Chamber of Shipping have published cyber security workbook for onboard ship use to support ships crew in case of cyber incident. There are checklists and guides how to protect, notice and respond to cyber exploits. (Eleni Antoniadou & Akshat Arora, 2020.)

4.6 Technical protection

Technical protection measures are a way to ensure that systems are resilient to cyber incidents. It is important that the officers keep the protective means such as firewall up to date and check that they are online all the time. Networks that are important for the vessel operations should be monitored and controlled such as:

- OT systems that grant remote access navigation systems
- Cargo loading, load planning, cargo, and container management systems
- Networks that grant access to guest

Nowadays many ships have crew Wi-Fi, this creates a risk to the vessel networks.

The crew's internet should have no connection to OT, nor should there be any connection with the ship's internet, which is used to process vital information onboard. Uncontrolled networks such as crew wi-fi should be considered as high-risk. (BIMCO et al., 2021.)

5 LEGISLATIONS AND INSURANCE

There is high lack of legislation in maritime cyber sector. Maritime organizations and shipping companies should take steps to safeguard shipping from emerging threats and vulnerabilities related to cyber security. Legal risk in cyber crimes includes contractual liability, third party liability, and potential regulatory breaches. Maritime Safety Committee meeting held on June 16, 2017, stated: "*There is an urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks"* (IMO, 2017). Maritime safety committee Resolution MSC.428(98) and MSC-FAL.1/Circ.3 are the up to date circulars as of now. Resolution MSC.428(98) important statement is that cyber risks must be addressed in existing safety management systems and to be verified in audits from January 1, 2021. MSC-FAL.1/Circ.3 gives high level recommendations on maritime cyber risk management. (IMO, 2022).

There is also The Guidelines on Cyber Security Onboard Ships published by BIMCO (2021) which gives good and profound information about the current situation in maritime cyber sector. BIMCOS guidelines are only instructions and most of the excellent work is not put into use until it becomes legislation. Cyber security clause produced by BIMCO obliges contractual charter parties to notify one of any cyber attacks. This is intended to address situations where company is hit by cyber exploits and is unable to accomplish its contractual obligations. (BIMCO et al., 2021.)

International Association of Classification Societies has released Recommendations on Cyber Resilience. Purpose of this publication is to provide technical recommendations to stakeholders, which would lead to more cyber resilient vessels. (IACS, 2020.) This publication is also just a recommendation for shipping companies. None of these publications have been approved by the International Maritime Organization and they state on their website: "*International Maritime Organization is not responsible for any external produced content."* Lack of maritime cyber security legislation is alarming and should be addressed quickly.

5.1 Insurance

Cyber incidents have high probability to lead to economic loss. It is estimated that 92% of the costs that result from a cyber attack are uninsured. (Clark, 2021). Currently there are no specific exclusions in Protection and Indemnity insurance, but constitute terrorism, war risks and hazardous or improper acting are excluded from P&I. Lack of cyber attack coverage on P&I club rules is alarming. There are some insurances that are intended for cyber exploits but due to limited data about insurance cases on court no established rules are applied. There are still some general rules when insurances apply certainly in cyber incident:

- Loss of life
- Personal injury
- Pollution
- Loss/damage to cargo or cargo handling equipment
- Business interruption or loss of production
- Loss of data
- Loss of reputation
- Legal costs

If these certain conditions are not met, the costs will be paid by the owner in full which just furthermore shows how important it is for the company to have cyber security at an excellent level. (BIMCO et al., 2021.)

Marine cyber endorsement Lloyd's Market Association 5403 have also been adopted by P&I clubs. The endorsement says that: "S*ubject only to paragraph 3, in no case shall this insurance cover loss, damage, liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus, computer process or any other electronic system*". (Lloyd's Market Association Marine Committee, 2019.)

Maritime cyber attack exclusion clause LMA 402 was published in 11 November 2019. This clause states that:

> *1. In no case shall this insurance cover any loss, damage, liability or expense directly or indirectly caused by, contributed to by or arising from:*
> *1.1 the failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system, or*
> *1.2 the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.*

The burden of proof falls on insured, who must show case inter alia that the motive behind the cyber attack was to damage solely insured or its property. (Lloyd's Market Association Marine Committee, 2019.)

P&I club gives example cases to get a better understanding about P&I cyber security insurance coverage. In the first one where cargo vessel was laden with cargo onboard and was late from loading port because ECDIS was infected with virus. Vessel was designed for paperless navigation and did not have paper charts. The source and means of infection are unknown and similar ransomware was infected to ships server and caused complete shutdown of the IT infrastructure. P&I Clause 15 states: *"In the event of loss of time from deficiency of men or stores, fire, breakdown or damages to hull, machinery or equipment, grounding, detention by average accidents to ship or cargo…. or by any other cause preventing the full working of the vessel, the payment of hire shall cease for the time thereby lost."* (London Class P&I, 2018). This placed vessel off-hire for a week and prevented it from sailing. Insurance would cover the off-hire event, legal costs and damage to cargo caused by delay. Whether member acted according to P&I rules would be central in the case. (ABS Group, 2020.)

In the second case hacker gained access to a shipowner's email system. Cyber hackers impersonated the shipowner leading to payments under the charterparty being directed to malicious actor bank account. At the same time shipping company's networks were infected with malware. Ships were also affected by the attack, and company paid the ransom.

The risks here are not covered by P&I because there is no third-party liability encountered in the commercial operation of the infected vessels. Legislative assistance and recover of lost funds would be done. (ABS Group, 2020.)

At last case malware is installed from USB stick by due to crew error. That causes loss of all navigation systems and causes the ship collision into the seabed, injury of one and death of two crew members. Here P&I rules apply because crew negligence is covered under P&I rules. Insurance works normally in this case and cover liabilities, expenses and costs that are subject to the incident. (ABS Group, 2020.)

6 CONCLUSIONS

High cyber security risks on vessels can be divided into two categories: First high threat is the OT systems that are connected to internet. Second high threat is technical characteristic of GNSS system and the alarming number of successful attacks on GPS using GPS spoofing.

Shipping companies should take security measures to make sure vessels positioning systems are up to date for modern cyber exploits. It is important for the company to not only look one individual system cyber security, but also to look the whole company cyber security, which should include all company members. It is important to understand that everyone the company works creates a risk to the company cyber security, this highlighted well in Maersk case.

Crew members in today's maritime industry have high number of duties already onboard so hiring a subcontractor for the cyber security should be mandatory for each company. Crew members should have all time available connection with IT workers if the attack occurs. Contact information must be in cyber security attack response plan and the plan must be accessible quickly. Cyber security should be thought within the company as an investment. Investing in crews' education is the most cost-effective way to mitigate risks related to cyber security. Every crew member onboard should go through course designed to educate staff about the malicious attacks.

OOW should be ready to respond and always verify the signal with other sources for the possible spoofing events of GNSS systems. Continuous growth in spoofing accidents and easily accessible spoofing devices online make it threatening and dangerous for safe navigation. Lack of security in navigation data makes GNSS out of date to respond on cyber threats. Due to these threats, it is important for the navigator to not rely on ECDIS and AIS information only.

More effective legislation and instructions from IMO are needed quickly to start protecting vessels from cyber threats.

IMO statement that after January 1, 2021, vessel Safety Management System should include effective cyber risk management system is step to right path, but more direct rules need to be set. Cyber security should be part of the training schedule on ships to ensure crew is educated about the new cyber risks to ships operations. Currently there is no requirements under Standards of Training, Certification and Watchkeeping for Seafarers but in ISM code it is stated that staff should be qualified in their tasks which includes cyber security. There is still a need to place cyber security training as a part of STCW Code according to my experience.

In insurance cases, we saw that P&I would not cover classic ransomware attack what could take place, for example from phishing emails. It is important that these cyber attacks are included in the company's insurance policies as they can have devastating effects on business continuity.

From my own experience, I have noticed cyber accidents highlighting traditional navigation and why paper navigation is still important for officers. However, due to the increasing use of ECDIS, it will not solve the problem

6.1 Future research

Future research should be targeted more towards cyber security of OT systems onboard and study today's ships, for example passenger vessels how their cyber security is organized. Alarming pace at which attacks are growing and succeeding towards OT on vessel should be studied more and it would be beneficial to see how current vessels are designed to address these threats. This should be done in cooperation with IT department to gain full access to vessels cyber security protection.

REFERENCES

ABS Group. (2020, October). *MANAGING CYBER RISKS AND THE ROLE OF THE P&I CLUB: AN OVERVIEW*. https://www.american-club.com/files/files/managing_cyber_risks.pdf Accessed 15.01.2022.

Androjna, A., Perkovič, M., Pavic, I., & Mišković, J. (2021). AIS Data Vulnerability Indicated by a Spoofing Case-Study. *Applied Sciences 2021, Vol. 11, Page 5015*, *11*(11), 5015. https://doi.org/10.3390/APP11115015 Accessed 12.01.2022.

BIMCO, C. of S. of A., Shipowners (INTERCARGO), I., International Chamber of Shipping (ICS), I. U. of M. I. (IUMI), O. C. I., & Marine Forum (OCIMF), S. B. A. (Sybass) and W. S. C. (WSC). (2021). *THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS Produced and supported by The Guidelines on Cyber Security Onboard Ships*. https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf Accessed 28.02.2022.

Bockmann Wiese Michelle. (2019, August 16). *Seized UK tanker likely 'spoofed' by Iran: Lloyd's List*. https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran Accessed 12.03.2022.

C4ADS. (2019). *Exposing GPS Spoofing in Russia and Syria C4ADS innovation for peace Above Us Only Stars COVER IMAGE LEGAL DISCLAIMER*. www.c4ads.org Accessed 05.03.2022

Cisco. (2018). *What Is a DDoS Attack? Distributed Denial of Service - Cisco*. https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html#~latest-ddos-trends Accessed 12.03.2022.

Cloudflare. (2022). *What is a distributed denial-of-service (DDoS) attack? | Cloudflare*. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ Accessed 28.02.2022.

Cyber Edge. (2017). *cyber-edge.com | 522: Connection timed out*. https://cyber-edge.com/wp-content/uploads/2017/06/CyberEdge-2017-CDR-Report.pdf

Duncan Parnell. (2020, June 11). *What's the Difference Between GPS Spoofing and Jamming?* https://www.duncan-parnell.com/blog/whats-the-difference-between-gps-spoofing-and-jamming Accessed 28.02.2022.

Eleni Antoniadou, & Akshat Arora. (2020). *Maritime Cyber Risk Management Guidelines Industry Expertise: Loss Prevention*. Accessed 12.03.2022.

IBM. (2020). *Cost of a Data Breach Report 2020*. https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf Accessed 12.03.2022.

IBM. (2022). *What is a cyber attack? | IBM*. https://www.ibm.com/topics/cyber-attack Accessed 16.3.2022.

IMO. (2017). *GUIDELINES ON MARITIME CYBER RISK MANAGEMENT*. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-

%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf Accessed 24.03.2022.

Imperva. (2021). *What is phishing | Attack techniques & scam examples | Imperva*. https://www.imperva.com/learn/application-security/phishing-attack-scam/ Accessed 28.2.2022.

Isaac R, & Porche III. (2020). *Cyberwarfare: An Introduction to Information-Age Conflict*. https://books.google.fi/books?id=3bzPDwAAQBAJ&pg=PA320&lpg=PA320&dq=infection+of+malware+with+usb+to+vessel&source=bl&ots=piPhoL6FUU&sig=ACfU3U3zRR55wn3HS1igTbvH3Vp8GwMjDQ&hl=fi&sa=X&ved=2ahUKEwj-5qXizbv2AhVCSPEDHSCpBMQQ6AF6BAgSEAM#v=onepage&q=infection%20of%20malware%20with%20usb%20to%20vessel&f=false Accessed 16.03.2022.

Kate Veale. (2022). *Virus vs Malware vs Ransomware: What's the Difference in 2022?* https://www.vpnmentor.com/blog/difference-between-malware-ransomware/ Accessed 15.01.2022.

Kordia. (2017, June 28). *NotPetya Attack: What You Need to Know and Do*. https://www.kordia.co.nz/news-and-views/petya-ransomware-attack Accessed 16.3.2022.

Lo Chirs. (2019, April 15). *Ship navigation risks: defining the threat of GPS spoofing*. https://www.ship-technology.com/features/ship-navigation-risks/ Accessed 12.03.2022.

London Class P&I. (n.d.). *London Class P&I and Defence rules*. Retrieved March 23, 2022, from https://www.standard-club.com/fileadmin/uploads/standardclub/Documents/Import/publications/rules/2017/2533539-london-class-pi-and-defence-rules-and-correspondents-2017-18.pdf#page=38 Accessed 28.2.2022.

Lord Nate. (2018, November 11). *What is Social Engineering? Defining and Avoiding Common Social Engineering Threats | Digital Guardian*. https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats Accessed 15.01.2022.

Louie Chris. (2017). *Better to be Lucky Than Good? After Not Petya, Shipping Company Maersk Saved by Power Outage — Chris Louie, CISSP*. https://www.chrislouie.net/blog/2018/9/10/better-to-be-lucky-than-good-after-not-petya-shipping-company-maersk-saved-by-power-outage Accessed 16.03.2022.

Proofpoint. (2021). *Human Factor Report 2021 - Cybersecurity During COVID-19 | Proofpoint US*. https://www.proofpoint.com/us/resources/threat-reports/human-factor Accessed 28.02.2022.

Security Magazine. (2020). *Maritime Industry Sees 400% Increase in Attempted Cyberattacks Since February 2020*. https://www.securitymagazine.com/articles/92541-maritime-industry-sees-400-increase-in-attempted-cyberattacks-since-february-2020 Accessed 11.03.2022.

Security.org Team. (2021, October 1). *America's Password Habits 2021 - Security.org*. https://www.security.org/resources/online-password-strategies/ Accessed 15.01.2022.

Stouffer Clare. (2021, December 8). *Password security + 10 password safety tips | Norton*. https://us.norton.com/internetsecurity-privacy-password-security.html Accessed 23.03.2022.

Todd Hymphreys. (2013, June 29). *UT Austin Researchers Spoof Superyacht at Sea*. https://cockrell.utexas.edu/news/archive/7649-superyacht-gps-spoofing Accessed 28.02.2022.

Jessica Scarpati & John Burke. (2021, September). URL (Uniform Resource Locator). https://www.techtarget.com/searchnetworking/definition/URL Accessed 02.04.2022.

Novatel. (2015). An introduction to GNSS. https://novatel.com/an-introduction-to-gnss Accessed 02.04.2022.

Julian Clark. (2021, March 12). Meeting the cyber threat challenge in the maritime industry – protection beyond regulation. https://www.maritimelondon.com/news/meeting-the-cyber-threat-challenge-in-the-maritime-industry-protection-beyond-regulation Accessed 07.04.2022.

Lloyd's Market Association Marine Committee. (2019, November 11). Marine Cyber Exclusion, Marine Cyber Endorsement https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA19-031-PD.aspx Accessed 08.04.2022.