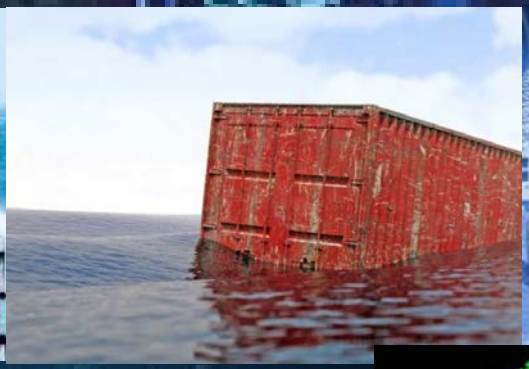
Cyber-Attacks: **The new type of piracy in the Maritime World**



UNIVERSITY OF PIRAEUS

DEPARTMENT OF MARITIME STUDIES

MASTER OF SCIENCE IN SHIPPING MANAGEMENT

Cyber-Attacks: The new type of piracy in the Maritime World

Maria Evelina Alifragki

Master Theses submitted to the Department of Maritime Studies of the University of Piraeus as part of the requirements for obtaining a Postgraduate Diploma in Maritime Management.

Piraeus

September 2019

Declaration of Authenticity

The person preparing the thesis bears the responsibility of fair use of the material, which is defined on the basis of the following factors: the purpose and character of the use (commercial, non-profit or educational), the nature of the material used (part of the text, tables, figures, images or maps), the percentage and the importance of the text, which uses relatively to the entire text under copyright, and the possible consequences of such use on the market or the overall value of the copyright text.

Maria Evelina Alifragki

Three Member Examining Board

This thesis was approved unanimously by the three-member Commission of Inquiry appointed by the “ΓΣΕΣ” of the University of Piraeus, Department of Maritime Studies, in accordance with the Management Regulations of the MSc in Shipping Management.

The Committee members were:

-Professor A. Artikis

-Professor Aggelos Pantouvakis

-Professor Georgios Danihl

The approval of the thesis by the Department of Maritime Studies, University of Piraeus does not imply acceptance of the author's opinions.

Acknowledgements

It is a great pleasure to acknowledge my deepest thanks and gratitude to Mr. Athanasios Martinos. Without him my dream for attending my postgraduate studies in the University of Piraeus would be impossible.

I would also thank my family, my friends and my managers for being by my side all this time. Their support were one of the part of my strength to do my best and combine my job's life with my personal life together with my obligations to the university.

I am also gratefully to the three-member committee and especially to my supervisor Professor Alexandros Artikis for his guidance and support throughout this research project.

I wish that the hard work for my master thesis will be obvious to everyone who wants to read it. There was a difficult time for me to prepare this document by reading all the subject related material and learn so many information from these.

Abstract

Title of Dissertation: Cyber-Attacks: the new type of Piracy in the maritime world

Degree: Master of Science

Nowadays, technology has grown rapidly, with the society and commerce following this evolution and digitalization too, as has shipping. The maritime industry and also the whole trade, all this time, have used a variety of systems, programmes and equipment. With this advantage, the maritime sector has reputational, economical and operational benefits. But there are also disadvantages, as the threats and cyber risks play significant role in the cyber security world. A variety of information and data are exposed in different internet platforms and networks. As a result, there is always in our minds the threat of a potential cyber-attack, after the attacks that were happened on important companies.

This research focuses on the cyber security, in general, in the whole maritime industry sector and how this subject is dealt with the Safety and Security ashore and onboard, from the view of the international maritime organizations. Moreover, the interesting parts in this research are the view of Cyber-attacks from the Insurance sector and the coverage that are able to offer or not, and also the fundamental part of Seaworthiness, how operates in every case.

In addition, there are companies that have already changed their procedures to be, as cyber secured as they can, to protect them from a cyber-attack and to prevent any vulnerability in the cyber world, a typical procedure is discussed below. Finally, safety, financial and environmental consequences in the industry are discussed together to conclude all this discussion, normally.

Keywords: Cyber security, Cyber-attacks, Threats, Risks, Safety, Security, Coverage, Seaworthiness, Vulnerability, Consequences.

Περίληψη

Τίτλος Διπλωματικής Εργασίας: Επιθέσεις στον Κυβερνοχώρο: ο νέος τύπος πειρατείας στον χώρο της Ναυτιλίας.

Βαθμός: Μεταπτυχιακό των Επιστημών

Σήμερα, η τεχνολογία έχει αυξηθεί ραγδαία, με την κοινωνία και το εμπόριο ακολουθώντας την εξέλιξη και την ψηφιοποίηση, όπως και η ναυτιλία. Η ναυτιλιακή βιομηχανία, αλλά και όλο το εμπόριο, όλο αυτό το διάστημα, έχουν χρησιμοποιήσει μια ποικιλία συστημάτων, προγραμμάτων και εξοπλισμού. Με αυτό το πλεονέκτημα, ο ναυτιλιακός τομέας έχει οφέλη από τη φήμη, τα οικονομικά και λειτουργικά. Υπάρχουν όμως και μειονεκτήματα, καθώς οι απειλές και οι κίνδυνοι στον κυβερνοχώρο παίζουν σημαντικό ρόλο στον κόσμο της ασφάλειας μέσα από αυτόν. Διάφορες πληροφορίες και δεδομένα εκτίθενται σε διάφορες πλατφόρμες και δίκτυα του διαδικτύου. Ως αποτέλεσμα, υπάρχει πάντα στο μυαλό μας η απειλή μιας πιθανής επίθεσης στον κυβερνοχώρο, μετά τις επιθέσεις που συνέβησαν σε σημαντικές εταιρείες.

Η έρευνα αυτή επικεντρώνεται στην ασφάλεια μέσα στον κυβερνοχώρο γενικά σε ολόκληρο τον κλάδο της ναυτιλιακής βιομηχανίας και στον τρόπο με τον οποίο αντιμετωπίζεται αυτό το ζήτημα με την Ασφάλεια στην ξηρά αλλά και επί του σκάφους, από την άποψη των διεθνών ναυτικών οργανισμών. Επιπλέον, τα ενδιαφέροντα μέρη αυτής της έρευνας είναι η άποψη των επιθέσεων στον κυβερνοχώρο από τον ασφαλιστικό τομέα και της κάλυψης που είναι σε θέση να προσφέρουν ή όχι, καθώς και το θεμελιώδες μέρος της Ικανότητας ναυσιπλοΐας, πώς λειτουργεί σε κάθε περίπτωση.

Επιπλέον, υπάρχουν εταιρείες που έχουν ήδη αλλάξει τις διαδικασίες τους, καθώς είναι ασφαλείς όσο μπορούν, για να τους προστατεύσουν από επιθέσεις στον κυβερνοχώρο και για να αποτρέψουν τυχόν ευπάθεια στον κυβερνοχώρο, μια συνηθισμένη διαδικασία που περιγράφεται παρακάτω. Τέλος, οι συνέπειες για την ασφάλεια, τις οικονομικές και τις περιβαλλοντικές επιπτώσεις στον κλάδο συζητούνται μαζί για να ολοκληρώσουν, ομαλά όλη αυτή τη συζήτηση.

Λέξεις-κλειδιά: Ασφάλεια στον κυβερνοχώρο, επιθέσεις στον κυβερνοχώρο, απειλές, κίνδυνοι, ασφάλεια, ασφάλεια, κάλυψη, αξιοπλοΐα, ευπάθεια, συνέπειες.

Table of Contents

List of Abbreviations

MTI: Marine Transportation Information

IRISL: Iranian Shipping Line

IT: information technology

OT: operational technology

CEO: Chief Executive Officer

VLCC: Very Large Crude Carrier

LMA: Lloyd's Market Association

NMA: National Management Association

P&I: Protection and Indemnity Insurance

IGPANDI: International Group of Protection & Indemnity Clubs

IMO: International Maritime Organization

SUA: Suppression of Unlawful Acts

SOLAS: International Convention for the Safety of Life at Sea

ISPS: International Ship and Port Facility Security

MSC: Maritime Safety Commitee

ISM: International Safety Management

SMS: Ship Management System

ISMS: information security management system

BIMCO: Baltic and International Maritime Council

CLIA: Cruise Lines International Association

ICS: International Chamber of Shipping

OCIMF: Oil Companies International Marine Forum

IUMI: International Union of Marine Insurance

ISO/IEC: International Organization for Standardization

IEC: International Electrotechnical Commission

NIST: National Institute of Standards and Technology

CIRM: Comité International Radio-Maritime

DNV: Det Norske Veritas

MOU: mobile offshore unit

UKAS: United Kingdom Accreditation Service

LOC: letter of compliance

LR: Lloyd's Register

ICT: Information and communications technology

ICC: International Chamber of Commerce

ABS: American Bureau of Shipping

FCI: Functions, Connections and Identities

B/L: Bill of Lading

eB/L: Electronic Bill of Lading

LOI: Letter of Indemnity

COSPAS-SARSAT: Search and Rescue Satellite Aided Tracking

GMDSS: Global Maritime Distress and Safety System

AIS: Automatic Identification System

LRIT: Long-Range Identification and Tracking system

VMS: Vessel Monitoring System

SAR: search and rescue

EPIRB: Emergency Position-Indicating Radio Beacon

LUT: Local Users Terminal

LEOLUT: low-altitude Earth orbit

GEOLUT: geostationary Earth orbit

LEOSAR: low-altitude Earth orbit

GEOSAR: geostationary Earth orbit

MEOSAR: medium-altitude Earth orbit

MCC: Mission Control Center

RCC: Rescue Coordination Center

SPOC: Search and Rescue Points of Contact

SART: Search and Rescue Locating Equipment

DSC: Digital Service Calling

NAVTEX: Navigational Telex

AOR-E: Atlantic Ocean-East

AOR-W: Atlantic Ocean-West

POR: Pacific Ocean

IOR: Indian Ocean

LES: Land earth Stations

MES: Mobile Earth Stations

NCS: Network Co-ordination Station

NOC: Network Operations Centre

GT: Gross Tonnage

MSI: Maritime Safety Information

GPS: Global Positioning System

VMS: vessel monitoring system

ERS: Electronic Reporting System

MUNIN: Maritime Unmanned Navigation through Intelligence in Networks

MASS: Maritime Autonomous Surface Ships

GDRP: General Data Protection Regulation

ICO: Information Commissioner's Office

NCSC: National Cyber Security Center

Terminology and Definitions

Cyber: refers to both information and communications networks. (NISTIR)

Cyber Risk or Cyber Crime: 'refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.' (IMO)

Cyber Security: refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cybersecurity strategies include identity management, risk management and incident management. (Techopedia)

Cyber Security Threat: A potential cause of a cyber incident that might exploit a vulnerability to breach cyber security and cause harm to systems and organizations.

Cyber-attack: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (NIST)

Maritime Cyber Security: A relatively new branch of cyber security that focuses on preventing cyber-attacks targeted at the systems aboard vessels and the maritime control systems.

Cyber Threat: An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss. Note: The specific causes of asset loss, and for which the consequences of asset loss are assessed, can arise from a variety of conditions and events related to adversity, typically referred to as disruptions, hazards, or threats. Regardless of the specific term used, the basis of asset loss constitutes all forms of intentional, unintentional, accidental, incidental, misuse, abuse, error, weakness, defect, fault, and/or failure events and associated conditions. (NIST)

Cyber Incident: Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or

the information residing therein. See incident. See also event, security-relevant event, and intrusion. (CNSSI)

Vulnerability: A weakness or flaw in the design, implementation or operation of a system that an attacker can exploit to reduce the system's information assurance.

Reliability: property of a system and its parts to perform its mission accurately and without failure or significant degradation (ISO/IEC 27036-3:2013)

Autonomous Shipping: The act of transporting cargo overseas via an autonomous vessel. The autonomous shipping chain includes ground transport to the ports, cargo handling at ports as well as transport overseas. The goal of autonomous shipping is to minimize the human input required to ship items.

Autonomous vessel: A ship that is unmanned and mostly self-navigating. It receives major navigation decisions through a satellite data link from a crew ashore if needed but can do navigational decisions itself by analyzing sensor and GPS data in a nor-mal situation.

Unmanned ship: ship that does not physically contain a human and is capable of controlled movement. Unmanned ship may be remotely controlled, supervised or fully autonomous.

1. INTRODUCTION

Nowadays, the maritime world is based on technology and automation systems, in order to successfully control offshore and ashore, the maritime trade around the entire world, in a more competitive way. In the last decades, the maritime industry has significantly modified, all of its processes, due to the arrival of the Internet world.

Technology has emerged as one of the biggest parts of our everyday lives, from our homes to our businesses and jobs. So, more and more digital development is required to become effective and vigilant. But, in every case as we will see below, in this research there are advantages and disadvantages to lead us in a decision.

Moreover, digitalization in the maritime industry has been proved that it is even necessary for the modern shipping companies even to the “traditional” ones. In recent years, a large number of applications have been developed and established in the maritime industry, operational technology and information technology are cooperate in the world wide trade system to increase the standards in every case.

However, if we consider the wide range of operations that take place every day around the world (for example in ports, lakes, rivers, canals, and open seas etc.) the risks become even bigger regarding safety and security in every part of the supply chain. Every electronic system is very vulnerable to cyber-attacks, in other word and most common, hacking. As the maritime history show us that a lot of cyber-attacks take place, sometimes with small impacts in the maritime trade, but sometimes with big enough impacts and accidents which lead and concern the maritime industry and maritime organizations to establish and consolidate high protection systems to minimize the risks or regulations in the maritime cyber area to protect every effective of not person/company/port/organization etc.

Cyber security is not just about preventing hackers gaining access to systems and vital information, potentially resulting in loss of confidentiality and/or control. It also addresses the maintenance of integrity and availability of information and systems, ensuring business continuity and the continuing utility of digital assets and systems. The insider threat from shore-based or shipboard individuals who decide to behave in a

malicious or non-malicious manner cannot be ignored. Ship owners and operators need to understand cyber security and promote awareness on this subject to their stakeholders, including their shipboard personnel (Hugh Boyes and Roy Isbell, 2017).

Cyber security threats is an issue that will concern the maritime sector and cyber-attacks are here to stay (MTI, 2015). Cyber security awareness has to be established in every sector around the maritime trade world, by strategic and to implement decisions from high trained and executive professionals to recognize every dubious movement in the cyber environment.

The biggest percentage of the world trade is carried out by the maritime industry. Every day, thousands of maritime companies compete with each other for a higher position in the worldwide maritime industry ladder. So, it is understandable that the competition may sometimes makes the need to protect against of cyber-threats or "weird" cyber movements, for information extraction regarding strategic movements and decisions or to provoke a financial loss in the context of competition.

2. MARITIME CYBER-ATTACKS - CASES

2.1 INTRODUCTION

While increased automation and artificial intelligence seem to open new routes for shipping, vulnerability of systems is another area of concern shipping has to cope with (Safety4Sea, 2018). Throughout, modern maritime history of the world, cyber-attacks have changed the way people think. After these attacks a lot of the maritime organizations have adopted and drafted laws and regulations to fit and protect third parties and any liability that arises after a cyber-attack. Cyber security is a fundamental issue that concerns a lot, has troubled the maritime sector during all these years. Some companies have taken serious steps to protect their employees and their systems, while other companies are still early stages. There is also the case of some companies that have faced cyber-attacks but chose to conceal the facts, for commercial reasons. It is an acknowledged truth that the maritime sector has created a competitive environment for each member within its "community". But there is a remarkable point that showcases the

solidarity amongst aforementioned as all its members ally with each other to protect and prevent any future, underlying danger.

2.2 SAUDI ARAMCO'S CASE

Saudi Aramco is one of the largest oil production companies in the world, it supplies the 10% of the world's oil and is one of "The New Seven Sisters", according to the Financial Times, meaning it is among the biggest and the most important national oil and gas companies, between based in countries outside of OECD, with 2018 revenues, approximately to $ 355.90 billion and with net profit at $ 111 billion. The State's economy is highly dependent on oil production, regarding the national economy. On the 15th of August of 2012, during the Islamic Ramadan (19/07/12 – 18/08/12), Aramco got attacked by a cyber virus named Shamoon. An inside investigation revealed that one of the computer technicians on Saudi Aramco's information technology systems team opened a scam email and clicked on a suspicious link. As a result, 35,000 computers, crashed or were partially strained, in a matter of hours. Suddenly, Saudi Aramco's supply was in big risk, without a way to pay the suppliers and gasoline tank trucks seeking refills had to be drawn away. The 17 days that followed the attack, the immediate measures that Aramco had taken with assistance with the IT professionals assistance were modify into a more paper-based system, not dependent on Internet access or phones etc. The corporation started giving her oil for free, to keep it flowing within Saudi Arabia, mainly for commercial reasons. Until this day, the hackers were not identified but Saudi Aramco has updated all of the company's systems and hired an executive cybersecurity team for extra protection of the company. Additionally, such an attack could lead a small or a middle-sized company to bankruptcy. Instead, after that incident, Saudi Aramco is such as powerful and independent company that no one could have imagined.

2.3 IRANIAN SHIPPING LINE'S (IRISL) CASE

IRISL is a government owned shipping company with a fleet of 115 ocean-going vessels and her plans are to be included in the top-ten shipping lines by the end of 2020. In the past, IRISL has been sanctioned by the U.S., UN, EU and other parties for its role in advancing Iran's nuclear and ballistic missile programs. In August 2011, IRISL suffered damages by a cyber-attack, compromising the entire fleet and shore-based systems. As a

result, the company lost all the internal communication network, suffered significant disruptions in operations, damaging all date related to shipping rates, loading, discharging, cargo information, date and locations of the entire fleet and client information and communication data were vanished. Consequently, nobody could know the right location of each container and the tracking of each one became more difficult and unpredictable. So a massive amount of cargo was delivered to wrong destinations or even lost.

2.4 PORT OF ANTWERP'S CASE

The port of Antwerp, in Flanders, Belgium is the second largest port of Europe, after Rotterdam, and the biggest players in the world in logistics, mobility, IT and supply chain management, with a big number of vessels of all kinds and types that operate every day in this area. In June 2011 and for a (2) two years period, until late of 2013, hackers based in Belgium, organized by a drug cartel, had compromised and took over the control of the terminals' system. Their well-organized plan was to release containers to their own truckers, without been seeing by the local port authorities and to remove all the specific data from the relevant databases, regarding the contraband containers. They had the ability to steal several amount of the cargo from the containers and sometimes to steal an entire container with all the belongings. When Belgian and Dutch police further investigated the case, they also discovered a ton of cocaine, guns, bullet-proof vests, and 1.3 million euros of cash in a suitcase. After the discovery, the national police and everyone who has been involved in this case, had to "dig" deeper to find out all the relevant details and plans regarding this criminal issue. Mr. Rob Wainwright, the director of Europol said "[The case] is an example of how organized crime is becoming more enterprising, especially online," Nowadays, the Port Authority of Antwerp has the AMARIS, the IT department for Antwerp Maritime Information Systems, to support and develop specific maritime and related applications and also to manage the computer park of the local port authority for avoidance such incidents in the future.

2.5 A.P. MOLLER-MAERSK'S CASE

A.P. Møller-Maersk is a Danish multi-industry company, widely known as Maersk, with activities in a lot of sectors such as, logistics, energy and transport, with revenues more than $ 35 million annually. On the 27th of June 2017, in Ukraine, a computer virus called NotPetya or Golden Eye started to spread in Maersk's company's network systems and 80,000 computer, worldwide. It was discovered that the virus entered into the system through an employee who clicked on an unidentified email. Moreover, the consequences were lots, several port terminals, run by APM, were struggling to operate normally, the dry cargo could not be delivered and no container would be delivered to the right destinations, because of the breakdown of some IT systems. Also, the cost of operations, cargo and container damages, as well as, upgrading their systems was extremely high. Further actions had to be taken by a Maersk's team of IT professionals, after cooperation and several meetings had taken place in Copenhagen, by the Maersk's CEO, Søren Skou, to face the consequences and solve immediately the problem. This incident resulted to Maersk being more careful in the internal cyber steps of the entire company, by adopting a new cyber security approach, by strengthening the IT infrastructure platform, including several services and meetings monthly, in addition to response and recovery plans, tested and planned in order to include new mitigation actions for future attacks. But the most remarkable one was that Maersk, after negotiations, has purchased cyber insurance for preventing a future cyber-attack and a potentially negative financial impact.

Furthermore, on September the 20th of the following year, several servers of the Port of Barcelona's security infrastructure were hit by a cyber-attack but apparently operations were not affected but showed the port's vulnerability to such incidents.

Five days later, the Port of San Diego's IT systems were disrupted by a ransomware attack that prompted investigations by the Federal Bureau of Investigation and the Department of Homeland Security (Michael Juliano, 2018).

Also, it has been reported that earlier in 2018, a criminal gang in Nigeria, targeting the global maritime industry, had been running multiple "business email compromise" scams

for hundreds of thousands of dollars. The group calling themselves “Gold Galleon” had been sending messages to infiltrate payments within shipping companies. Among the victims was a South-Korean and a Japanese shipping company (Safety4Sea, 2018). The maritime world, after all those incidents, started to compare them all together and face them like a traditional piracy’s incidents.

2.6 AUSTRALIAN CUSTOMS AND BORDER PROTECTION SERVICE AGENCY’S CASE

In 2012, Australia faced a cyber-attack common to IRISL’s case. Australian Customs and Border Protection Service Agency, the Australian federal government agency responsible for the security and the managerial prospects of the Australian borders, was attacked by hackers, working for a criminal syndicate, compromising the cargo system in order to know and control which shipping containers were suspected by the port and customs authorities or police, so as to predict and release the contraband containers in the right time. Seemly though, Australia was hackers’ target for many years before that attack, with a lot of cyber-events and a highlight on this year. Half of the Australians (almost 10 million) have been victims of cyber-attacks, in the first quarter of 2019 (1st January 2019 to 31st March 2019) with a 215 data breach notifications during this period.

In 2014 and 2015, many security firms faced cyber-problems. As a result, a number of vulnerabilities emerged from specific fishing operations targeting in specific maritime companies to breach Coast Guard IT systems.

2.7 CLARKSON PLC’S CASE

Clarkson Plc based in London, with offices all over the world, like Dubai, Singapore, Athens, Geneva, Oslo, Switzerland, Oslo, Houston etc. operate in several sectors, as broking, financial, support and research. On the 7th of November 2017, an unauthorized third party have entered Clarksons’ computer systems in United Kingdom by copying various important data and then asking for ransom money to return the “stolen” data. It was later discovered that this unauthorized third party gained access from a single, isolated user account, from the UK office collecting data for a six month period, from 31st

of May 2017 to 4th of November 2017. Moreover, some of the stolen data were contact details, passports, payment cards, date of births, bank accounts, security information, etc. Clarksons have immediately started investigations and took further steps by cooperating with law enforcement and forensic investigators. Thankfully, all the breached data were restored and the responsible user had to be fired. Sometimes the "problem" is initiated from inside and not from an outside source, so every company has to choose the best and the most reliable person for the company and, of course, convince and inspire that they are working towards the same purpose and the same result and protect their company against criminals and attacks.

3. CYBER-ATTACKS' COVERAGE

3.1 INTRODUCTION

The maritime cyber security is an issue that concerns a lot the shipping world and, consequently, the companies that are related to the coverage of any damage or loss caused by a cyber-attack, such as insurance companies, reinsurance companies and P&I clubs.

As the modern history of the maritime industry has shown, the number of cyber-attacks have been increased. To our knowledge, the hackers' target mostly the offices of shipping companies and no, the vessels. But this does not mean that vessels are no or less risk regarding cyber-attacks. Just imagine how catastrophic it would be, if hackers could have the entire control of a vessel. For example, if hackers deliberately navigate a vessel collide into another vessel or into a dock or into a reef or if hackers use a vessel as a mean to obstruct the entrance of a river or river port (port of Houston, port of Vienna, etc.) so as other vessels cannot enter or leave, this would result to boycott the trade in the area. So, many questions arise regarding the cyber insurance coverage and the liabilities of all the parties that are involved whenever a cyber-attack occurs.

Cyber risks cover a wide array of risks and types of loss, such as damage to objects, operating loss, theft, loss of immaterial rights, data loss and costs for data recovery, costs bearing court costs and carrying investigations by the authorities. In reality, the risks and types of losses that may occur from cyber-attacks are not covered by traditional insurance products. So, there is a need to develop new insurance products (Danish Maritime Authority, 2017)

3.2 INSURANCE COMPANIES

There are now over 60 companies in the UK, who market specific cyber insurance policies, and over 70 in the USA. However, whilst there may be certain commonality in the name of the policy and some of the risks covered, it is important to bear in mind, as always, that the devil is in the detail. Not all insurance providers offer the same things and the wording is usually inaptly put together (HFW, 2016). The risks regarding a potential cyber-attack are many, with a massive amount of money that the insurers have to cover for any damages. As a result, many underwriters want to exclude or avoid any liability. So, in a lot of marine insurance contracts, it is accepted the Institute Cyber Attack Exclusion Clause-Cl.380 (10/11/2003):

1.1 Subject only to clause 1.2 below, 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 or process or any other electronic system.

1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

However, it is unclear whether are considered the physical damages on the property or cargo or the environment after a cyber-attack. It can be difficult to understand whether the loss or damage has been caused by an excluded peril, because the cl.380 does not exclude loss, damage or liability resulting from an unintentional system malfunction (OECD, 2017).

Unfortunately, this clause was drafted 16 years ago, when the electronic systems in the maritime industry were still in early stages and especially the internet systems offshore and ashore. Also, the policies in every company or sector were different. In 2019, the maritime industry and all the other sectors that coexist on a daily basis, rely almost exclusively on the electronic systems, so, the market should review this clause (cl.380). Nonetheless, the insurers know the strength of the clause and have to consider the consequences under the new updated or revised exclusion clause and its content.

On the other hand, the Cl.380 is not the only exclusion clause, there is also the Terrorism Form T3 LMA3030 Exclusion 9: “Loss or damage by electronic means including but not limited to computer hacking or the introduction of any form of computer virus or corrupting or unauthorized instructions or code or the use of any electromagnetic weapon. This exclusion shall not operate to exclude losses (which would otherwise be covered under this Policy) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.” It was drafted some years later and includes a cyber-attack in the context of terrorism, but it is very close to the Cl.380. Also, the Electronic Data Exclusion NMA2914/15: “…This Policy does not insure, loss, damage, destruction, distortion, erasure, corruption or alteration of ELECTRONIC DATA from any cause whatsoever (including but not limited to COMPUTER VIRUS) or loss of use, reduction in functionality, cost, expense of whatsoever nature resulting therefrom, regardless of any other cause or event contributing concurrently or in any other sequence to the loss….” Alternatively, there is the NMA 2912 (Clarification clause) and 2928 and although, the NMAs apply more in non-marine property policies, it doesn’t fill the legislative gap of “cyber risk gaps” regarding the insurance coverage, even though it is not at the extend as the Cl.380 does. In other

respects, every insurance company can apply an Advanced Cyber Exclusion Clause, drafted by them, under negotiations between their customers and the underwriters.

3.3 PROTECTION AND IDEMNITY INSURANCE (P&I Clubs)

Marine insurance companies mostly provide, the well-known “hull and machinery” coverage for ship-owners and cargo coverage for cargo owners. On the other hand, P&I Clubs provide coverage mostly for third-party liabilities that a marine insurance company partially covers or does not cover at all, for ship owners, ship operators and charterers. Some examples are: environmental pollution, a carrier’s liability for damaged cargo, a ship owner’s liability after a collision or a contact, etc. The coverage for a cyber-attack event can be controversial for a P&I club, because such an attack on a vessel could lead to a third party liability without that meaning that a P&I Club covers every liability or ship owners’ risks. The International Group of Protection & Indemnity Clubs (IGPANDI) and every member of this Group (13 members), incorporate a “paramount clause” or the Institute Clause Cl.380. But, according to Mr. Tony Mayle “The effect of this exclusion (cl.380, 1.2) in a marine hull insurance policy is unclear. In the UK, it has not been tested at law; therefore, any view is based on our understanding of how the exclusion language may be interpreted by insurers.”

Here below, we can see the coverage (or not) for a cyber-attack for every P&I club that is a member of the IGPANDI and what they offer to their members:

- The American Steamship Owners Mutual Protection and Indemnity Association, Inc.: they do not incorporate the Institute Cyber Exclusion Clause (cl.380) to their contracts.
- The Britannia Steam Ship Insurance Association Limited: under their recommendations, they do not incorporate any Exclusion Clause regarding a cyber-attack.
- Gard P&I (Bermuda) Ltd.: they incorporate the Institute Exclusion Clause (Cl.380).

- The Japan Ship Owners' Mutual Protection & Indemnity Association: they divide cyber risks into internal and external. The Japanese Club does not provide coverage for internal cyber risk according to the Rules. They have a paramount clause which refers to: “This clause shall be paramount and shall override anything contained in this insurance inconsistent therewith: 1.2 the use or operation, as a means for inflicting harm, of any computer virus."
- The London Steam-Ship Owners' Mutual Insurance Association Limited: they incorporate the Institute exclusion Clause (Cl.380) too.
- The North of England Protecting & Indemnity Association Limited: under their Rules, they exclude the damages that occur because of the lack of computer antivirus protection, so every liability.
- The Ship-owners Mutual Protection & Indemnity Association (Luxembourg): they incorporate the Exclusion Clause (Cl.380) and also they apply their Clause: “CHEMICAL, BIO-CHEMICAL, ELECTROMAGNETIC WEAPONS AND COMPUTER VIRUS EXCLUSION CLAUSE which refers to: “This clause shall be paramount and shall override anything contained in this insurance inconsistent therewith: 4.1 In no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from 4.3 the use or operation, as a means for inflicting harm, of any computer virus. 4.4 Clause 4.3 shall not operate to exclude losses (which would otherwise be covered under the terms of this policy) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.”
- Assuranceforeningen Skuld: they incorporate the Institute Exclusion Clause (Cl.380), same as other P&I Clubs.
- The Standard Club Ltd: according to their rule 4(b), 5.17(2) and 6, which refers to the exclusion of any liability that arises from any computer system, any computer programme/software or any electronic system.
- The Steamship Mutual Underwriting Association (Bermuda) Limited: they incorporate the Exclusion Clause (Cl.380) under their Rules too.

- Sveriges Ångfartygs Assurans Förening / The Swedish Club: according to their Rules (Rule 2) they exclude any liabilities, costs and expenses caused by using a computer or a computer system and inflicting damage (Maritime Labour Convention (2006) Extension Clause).
- United Kingdom Mutual Steamship Assurance Association (Bermuda) Ltd: they incorporate the Exclusion Clause (Cl.380).
- The West of England Ship Owners Mutual Insurance Association (Luxembourg): they incorporate the Exclusion Clause (Cl.380), according to their rules regarding Paperless Trading and Maritime Labour Convention Extension Clause 2016.

3.4 REINSURANCE COMPANIES

Reinsurance coverage is used to increase market capacity by eliminating risks in the international markets, but mostly to eliminate the Underwriters' liability to any risk on the amount that they want to get rid of it.

Nowadays, if a company's cyber security does not operate in high standards the risk arising are enough to face a cyber-attack. Reinsurers want their customers to work on their cyber resilience, by constantly encouraging them and supporting them with the best practices through risk transfer and premiums. Insurers hold data for every old customer, especially for their business plans, their assets, Cyber Risk Management Policies and Third Party Liabilities Policies. They take into consideration every step that their customers have to do in order to be protected by any cyber risk.

Marine reinsurance companies may or may not use an exclusion clause like the P&I Clubs practice, upon the negotiations with their clients. "Reinsurers may rely on a warranty from the Primary Insurer to apply exclusionary language on each and every original policy." (Swiss Re, 2015). The marine reinsurance market is acting rather differently than any other and sometimes choose to move towards and possibly another way, after the 1st of January 2021, the maritime world will see the grey points of marine insurance policy and the kind of coverage after a cyber event, making it clearer than now.

But until then, the situation remains the same and confusing to each member of the maritime sector.

3.5 HIJACKING

In a weird way, the maritime industry as well as the marine insurance market sometimes, examines the incident of a cyber-attack as a hijacking issue. According to them these two meanings are linked.

Moreover, due to cyber-attacks on the various systems installed on on-board maritime vessels or structures, attackers were able to control these targets, with a number of different outcomes. For example, navigation and propulsion systems may be compromised either with false data, interference or by encrypting key files or system components.

According to a report issued by the International Criminal Police Organization in the years between 2005 and 2012, 179 ships were hijacked off the coast of Somalia and the Horn of Africa. The average ransom paid was $2.7 million, with ordinary pirates receiving $30,000 to $75,000 each and bonuses paid to those who brought their own weapons or were first to board the ship, with approx. an 85% success rate. Whilst the success rate cannot be generalized to other forms of hijacking, it does indicate a willingness on the part of the industry to pay which is of interest to criminal elements (MTI, 2019).

Ransomware has been common to traditional computing systems, as well as mobile devices, and could be adapted to the maritime domain. McAfee found that Ransomware is on the rise once again, with a 165% increase on new Ransomware, in the first quarter of 2015 (McAfee, 2015) showing that it is a highly profitable and growing sphere of criminal activity. Alternatively, a compromised ship may be guided by a hacker to crash into another target, either to destroy the ship or another desired target. This attack is viable against other ships, oil rigs, as well as some bridges and possibly some land-based structures, depending on the situation. Although no such events have occured, given the current level of potential attacks on maritime vessels, it does not seem impossible. For

example, (although not the same scenario) there have been reports of an oil rig being shut down after being overwhelmed with malware in 2010. Luckily, the rig was shut off before a possible well blowout, preventing oil spills and an explosion. However, removing all the malware from the rig took 19 days, costing the company in losses approx. up to $700,000 US each day (Shauk, 2013). Similarly, hijacking ships containing bio-hazard material, such as dangerous chemicals, or causing oil rigs to explode could heavily damage the environment, polluting the area, destroying other valuable resources, and harming the local economy (Tam, Papadaki, Jones, 2012).

Other past maritime incidents that were considered as cyber security incidents show us that the meaning of cyber-attacks and hijacking sometimes are the exactly same thing:

- The hijacking of the cruise ship SS Santa Maria, in La Guaira (Venezuela), 23 January 1961.

- The hijacking of the cargo ship Anzoátegui, off the Venezuelan coast, 12 February 1963.

- The hijacking of the cargo ship SS Columbia Eagle, 14 March 1970.

- The hijacking of the Italian cruise ship Achille Lauro, on 7 October 1985, was a significant actual terrorist act, led to a change from IMO the United Nations General Assembly.

- The hijacking of ferry MV Avrasya, in the port of Trabzon in Turkey, 16 January 1996.

- The attack on the Navy ship USS Cole, in the port of Aden in Yemen, 10 June 2000.

- The attack on the oil tanker SS Limburg, in the Gulf of Aden, off the coast of Yemen, 6 October 2002.

- The attack on the ferry SuperFerry 14, in the Philippines, 27 February 2004.

- The attack on the oil tanker VLCC M/V M. Star, in the Persian Gulf, 27 July 2010.

4. MARITIME ORGANIZATIONS

4.1 INTRODUCTION

Nowadays, the maritime global sector is based on digitalization, integration of operations and automation. According to the maritime trade history, many incidents have taken place all over the world in different places and years, each one having different target, leading to environmental or financial damages and costing human lives. So, the global organizations had to take actions and to create regulations, including them in the maritime legal framework, factoring in regulations regarding the maritime cyber security, both offshore and ashore. That is because the damages, differ on every situation, after a cyber-attack.

So on this chapter, all these organizations, profit or non-profit acting on the common interest of the protection of every company that will be possibly targeted, are accumulated to be examined. The most important organization, obviously, is the International Maritime Organization and the Guidelines on Cyber Security onboard Ships, an example of the cooperation the maritime industry is able to accomplish to face every problem or incident. Last but not least, there are Guidelines of another maritime organizations as BIMCO, ABS, DNV, Lloyd's, etc. So, there is a need for change and awareness, regarding the cyber security, the threats and the risks for these unknown "cyber paths".

4.2 IMO AND MARITIME CYBER SECURITY

The International Maritime Organization has been established since 1959, with its headquarters in United Kingdom, with 174 member states and three associate members in the maritime world, such as the United Nations' regulatory body, responsible for the safety of life at sea and environmental protection, with a big number of regulations and conventions until now.

According to the new security challenges that the maritime world suffered and concern the whole industry, the IMO had to act on behalf of all, in order to deal with the maritime cyber threats and make the international maritime trade as safe as possible.

Nevertheless, the IMO has been present for years now. On the 20th of November 1985, the IMO adopted the resolution A.584 (14) on Measures to prevent unlawful acts, which threaten the safety of ships and the security of their passengers and crews, after the terrorist incident on the Italian cruise ship Achille Lauro, on 7 October 1985. Also on 26th of September 1986, the IMO issued, the MSC/Circ.443 on Measures to prevent unlawful acts against passengers and crews on board ships by studying the threats.

The case of Achille Lauro triggered other conventions and gave the initiative for other regulations, such as the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA), March 1988, which extends the provisions to unlawful acts against fixed platforms located on the Continental Shelf, through the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988). Currently, 196 states ratified the 1988 Convention (SUA), corresponding to 94% of the world merchant shipping tonnage, and 154 states have ratified the 1988 Protocol. Also, important amendments regarding the 1988 SUA Convention were adopted by the Diplomatic Conference on the Revision of the SUA Treaties held from 10 to 14 October 2005. After September 1st 2001 and the terrible attack in USA, on the 20th of November 2001, the IMO Assembly resolved the A.924 (22) on the Review of measures and procedures to prevent acts of terrorism which threaten the security of passengers and crews and the safety of ships and reduce the threats and risks on vessels, crew, passengers, cargo, etc.

Moreover, on December 2002, IMO and the SOLAS 2002 Conference adopted some amendments on the International Convention for the Safety of Life at Sea (SOLAS), 1974, by creating the new International Ship and Port Facility Security (ISPS) Code, which contains recommendations, requirements and detailed security-related requirements for Governments, port authorities and shipping companies. But in 2012, IMO published the IMO Guide to Maritime Security and the ISPS Code for convenience and assistance of IMO's members. In 2014, the IMO successfully delivered 47 activities

around the world, making maritime security increasingly one of the largest capacity building programmes in the Organization.

Also, on the 16th June 2017, The Maritime Safety Committee, issued the Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems to encourage administrations to ensure that cyber risks are properly addressed regarding safety management systems, no later than the first annual verification of the company's Document of Compliance after 1 January 2021, (The Maritime Safety Committee, 2017).

After the 1st of January 2021, cyber risks and threats will have to be addressed through the Ship Management System (SMS) under the ISM Code. Last but not least, on the 5th of July 2017, the Organization also adopted the *Guidelines on maritime cyber risk management* MSC-FAL,1/Circ.3, which include high-level recommendations on maritime cyber risk management to develop cyber security systems in every company, around the shipping world and also introduce other guidance and standards from The Guidelines on Cyber Security Onboard Ships by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI or ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements by the International Organization for Standardization (ISO), which provides requirements for an information security management system (ISMS). The International Electrotechnical Commission (IEC) or United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework), assists companies with their risk assessments by helping them understand, manage and express the potential cyber risk threat both internally and externally. And also, the UK National Cyber Security Centre-Guidance.

4.3 BIMCO AND MARITIME CYBER SECURITY

The Baltic and International Maritime Council (BIMCO) is the largest international shipping association, with approx. 1,900 members, members being ship owners, managers, brokers, agents and operators, in more than 120 countries, with headquarters in Bagsværd, a town near Copenhagen, in Denmark. BIMCO has always had the vision “to be the chosen and trusted partner to provide leadership to the global shipping industry”.

BIMCO has records on a lot of incidents on vessels, with blackouts and malfunctions in radar and other related systems, as a result of unforeseen difficulties with a software update. In February 2016, BIMCO published “the Guidelines on Cyber Security Onboard Ships”, produced and supported also by CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL. This document was created to guide ship owners and operators how to protect their companies under the cyber security and cyber safety recommendations, to access their operations and find procedures to strengthen cyber resilience on board their ships. The fully updated Version 3, which has been published in December 2018, includes the requirement to incorporate cyber risks in the ship’s safety management system (SMS); more detailed information related to the risk assessments of operational technology (OT); increased guidance for dealing with the risks in the ship’s supply chain; case studies of verified cyber incidents onboard ships to highlight and illustrate potential problems. For the first time, in the maritime world, this version mentions and explains in detail every aspect and information regarding the types of cyber threats and cyber-attacks, every stage of any hypothetical attack, the vulnerabilities, the levels of potential impact, every process and phases in risk assessment, the protection tools required and plans regarding cyber security, as well as the processes and recovery plans after a cyber-attack. It is BIMCO’s and CIRM’s Comité International Radio-Maritime) goal that everyone involved in producing and maintaining software for shipboard equipment use this standard (Rasmus Nord Jorgensen, 2017).

Title: Cyber risk management approach as set out in the guidelines.

Source: “the Guidelines on Cyber Security Onboard Ships”.

4.4 DET NORSKE VERITAS (DNV GL)

DNV GL is the largest classification society in the world, providing services for approximately 13,500 vessels and mobile offshore units (MOUs) and an international accredited registrar, also called an accredited certification body (CB). Its headquarters are Høvik, a suburban area in the Oslo metropolitan area, in Norway. The

DNV is organized in five different domains, in Maritime, in Oil & Gas, Energy, in Business Assurance and in Digital Solutions.

DNV GL - Maritime has been improving services for safety, quality, energy efficiency and environmental performance of the global shipping industry, across all vessel types and offshore structures. As DNV GL states: “Cyber security is part of the ISM Code, effective from 2021, ensuring it will be part of a regulatory agenda in future”. DNV GL uses a systematic approach to assess the cyber security of vessels and their interaction with land-based management (DNV, 2019). “Whether in machinery, navigation or communication systems, programmable control systems are a longstanding and essential part of ships and offshore units, but the increasing integration and connectivity of these systems represents an ever-larger target for cyber-security threats,” Knut Ørbeck-Nilssen, CEO of DNV GL – Maritime said.

DNV’s plan is to combine the IT traditional system approach collaborating with a team of experts, with modern knowledge, thinking and experience in cyber security risk management, maritime operations and the human factor for the specific needs maritime industry has. So, their services and solutions, regarding the issue of maritime cyber security addressed to IT and OT systems and their professionals are:

- *Recommended practice “Cyber security Resilience Management (for ships and mobile offshore units in operation)”:* In September 2016, DNV published this document to get the word out on the risks and vulnerabilities of the cyber security and check and monitor every aspect in the maritime cyber environment, as practice for cybersecurity risk assessment.

- *Cyber security assessment:* Through an App on MyDNVGL, DNV’s professional team cooperates with every company’s onshore personnel and offshore crew to scrutinize every aspect on specific business areas and address your cyber security risks via various levels of assessment. It is rather remarkable that the 15 minutes questionnaire focuses on technical, security and etc. mechanisms and provides results immediately for the cyber security condition of each company.

- *Cyber security enhancement:* DNV helps every client close every cyber security gaps by creating elaborate plans and organized procedures, based on a systematic assessment.

- *Penetration testing:* DNV offers a penetration testing in order to ensure that the clients' systems are well protected, and the robustness of their barriers ensure that their assets are well secured too. The UKAS accredited Testing Laboratory, no.9334 provides these services including: New Product/System Testing, Common Criteria, Commercial Product Assurance and Business Vulnerability Assessment.

- *Verification for newbuilds:* DNV provides a third-party verification of cyber security requirements throughout the new build project life cycle and issue a letter of compliance (LOC). Moreover, in June 2018, DNV GL and RCL's maritime cyber security teams have published the following: "A proposed approach applied to modern cruise ship newbuilding", a paper to help owners, yards and vendors minimize every potential risk or threat of cyber-attack during newbuilding. The most remarkable on this paper is the analysis of two hypothetical cyber-attacks and their point of view.

- *Verification for ships in operation:* DNV provides an assessment of their clients' vessel's on-board cyber security and issue a LOC.

- *Training:* DNV offers and trains their clients on topics like management, technical and hacking lessons. The DNV's provides an e-learning alternative that can be performed on board to facilitate the crews but also in the office.

- *ISO/IEC 27001 preparedness:* DNV GL Maritime assesses the existing documentation to help companies prepare for certification. Also, in September 2016, DNV has drafted their rules (RP) "Cyber security resilience management

for ships and mobile offshore units in operation" to help and prepare everyone for the certification and its requirements and practices.

- *Certification:* DNV GL Business Assurance certify against ISO/IEC 27001 and ISO 22301.

It seems that DNV GL want to provide good and updated services to their customers. So, maybe in the view of competition, there will be another "competitors or players" who want to be like DNV GL.

4.5 LLOYD'S REGISTER

Lloyd's Register Group Limited (LR) is an old maritime organization with headquarters in London. Lloyd's started in 1760 with a wide range of customers around the world until today, with basic aims on protecting property, life and the environment. They offer services in the sectors of technology, business and maritime classification society. Nowadays, maritime cyber security issue is of high importance level for Lloyd's Register. For that reason, Lloyd's Register (LR) and a Lloyd's Register Company, Nettitude, cooperate to protect every client from any cyber-attack, by making use of helpful business and cyber tools, like training, auditing, penetration testing, managing cyber security services, etc. They also offer services as Cyber security procedures' definition, Risk or Threat assessment, Cyber security procedures, onboard audit and vulnerability assessment or penetration testing for preparing for Tanker Management Self-Assessment and assessing compliance to the BIMCO guidelines.

Source: the official website of Lloyd's Register, "Lloyd's cyber security assurance services".

LR's Marine & Offshore Director, Nick Brown, commented: "We understand that cyber security is essential to our clients' business, but something they do not want to impact or complicate their day-to-day operations. We will work with our clients to develop a cyber risk management plan specifically tailored to their business and operational needs, with the aim to embed cyber security seamlessly within their organization."

In February 2016, Lloyd's published the first section of guidance on cyber-enabled ships: "Deploying Information and Communications Technology in Shipping – Lloyd's Register's Approach to Assurance", describing and analyzing the technological systems and their implications. In each section, there are references on the Lloyd's Rules the ISO and IEC Standards, which helps all the stakeholders in the cyber-enabled ship market to combine and understand all the requirements of the Information and communications technology (ICT) systems.

On July 2016, Lloyd's Register published the first version of a guidance document related to Cyber-enabled ship, "Cyber-enabled ships: ShipRight procedure – autonomous ships", a very innovative issue with a detailed technical and systematical approach for Lloyd's Register's (LR's) framework, for accepting cyber technology at various levels of autonomy, from ships with the most basic decision support tools, to vessels that are fully autonomous, identifying the assessments, processes and considerations that need to be thoroughly followed (Lloyd's, 2016). On December 2017, a new version 2.0 was published "ShipRight procedure assignment for descriptive cyber notes for autonomous & remote access ship". Every updated version of their guide shows that their stakeholders and the maritime world, in general, that Lloyd's is an organization that wants their customers fully protected from any threat and up to date on the subject of cyber-attacks.

While the issue of cyber-attacks in the maritime industry has a big and important dimension for every country and state, Greece is a different case as it is a country with a variety of ship owning and management companies that have a big impact in the shipping economy. LR's Elisa Cassi stated: "As cyber threats continue to increase in the marine industry, it is our mission to ensure that our clients never make the headlines for the wrong reasons. Whilst it's impossible to eliminate cyber threats, implementing the right strategy, education and services covering both information and operational assets will dramatically reduce the risk of a breach, and the associated operational and safety risk as well as reputational and financial impacts. No business can make itself impregnable. What it can do, however, is seek to temper any attack on its critical business drivers by creating a scalable security posture." (March, 2019)

4.6 INTERNATIONAL CHAMBER OF COMMERCE (ICC)

The International Chamber of Commerce is the largest, most diverse business organization in the world. The ICC was founded 100 years ago, in 1919 and its International Court of Arbitration was formed in 1923, with headquarters in Paris (France) with millions of members in 100 countries all over the world and three main activities rule setting, dispute resolution and policy advocacy. Moreover, ICC has four

primary governing bodies, the leading governing body, the executive board, the international secretariat and the finance committee. Also, a lot of ICC's networks of committees and professionals from all sectors, have the duty to inform all the members for all the issues that affect their industries. ICC's mission is: "*We make business work for everyone, every day, everywhere*. Everything we do at ICC aims to promote international trade and investment as vehicles for inclusive growth and prosperity. From resolving disputes when they arise in international commerce to supporting global efforts to streamline customs and border procedures, we support multilateralism as the best way to address global challenges and reach global goals…" ICC wants every member to understand the high importance of indemnifying every risk that regarding cyber security and the threats it poses to their information systems indeed. Everyday many companies face challenges in their networks because their systems are threatened. Also, many of this companies have already reported suspicious bad movements to their cyber environment. Thus, ICC has listed some of them to protect each of the ICC's members by asking every company in daily research and report for every criminality movement.

As a result, ICC has prepared the ICC Cyber Security Guide for business, in 2015, which was inspired by the Belgian Cyber security guide. This guide was created to help business management of small and large organizations interact with their information technology managers and guide them into the development of cyber security risk management practices (ICC, 2015). The most vital aspect of this is that its content is composed by actions, steps and procedures that could encourage every member to face the issue of cyber security and the potential cyber-attack without causing disturbance in their companies.

In addition, there is a useful questionnaire, the self-assessment questionnaire, which is presented as a tool to help the management of each company for evaluating their strengths and weaknesses regarding their cyber resilience capabilities.

Another very important part of ICC is the Incoterms Rules. The last version of the Incoterms Rules was releases in 2010 and the business world has dramatically changed since, thanks to advancements in new software and technology. Manual procedures that

were common practice over 10 years ago, are continually being replaced by new digital supply chains (Ben Thompson, 2019). Although the Incoterms 2020 has not been published yet, ICC's members are focusing on the issue of cyber security and cyber-attacks in the world trade and especially in the maritime industry. It is considered that the Incoterms 2020 drafting committee will work along with cyber-security companies and experts that will prioritize potential security threats and vulnerabilities of participants, stakeholders and agents in the international trade. They will consider the introduction of technologies and capabilities that will eventually significantly minimize security and privacy concerns (Trade Finance Global, 2018).

4.7 AMERICAN BUREAU OF SHIPPING (ABS)

The American Bureau of Shipping (ABS) is a maritime classification society with headquarters in Houston, Texas (U.S.A.). ABS was founded in 1862, present for more than 150 years and has been promoting the security of life and property and preserving the natural environment. ABS has already 200 offices in 70 countries, around the world, with a wide range of network of surveyors, engineers, technical specialists and support staff, including experts on the cyber environment, to achieve their clients' missions, efficiently.

The cyber experts of ABS advanced solutions under their Cyber security program, have chased the traditional view of risks and created an innovative approach that produces a measurable risk index, the FCI Cyber Risk™ equation, the first of its kind in the maritime industry, which also supports compliance with the IMO's requirements via the IMO's guidelines. The ABS FCI Cyber Risk™ Methodology was developed following a two-year research contract with the Maritime Security Center—a U.S. Department of Homeland Security Center of Excellence—led by Stevens Institute of Technology and including the US Department of Defense (ABS, 2019). The basic aim was to help the clients to identify and count every risk and threat based on the FCI Cyber Risk equation which are:

Functions = mission critical systems such as navigation and propulsion, software that control machines on assets.

Connections = digital networks connecting Functions, nature and number of digital interfaces indicating cyber security complexity.

Identities = people or digital devices that can access these connections, or send or receive data by means of digital interfaces.

As a result, every client will be able to face every threat that is subjected to cyber security, (like something mathematically countable) and help them to invest on cyber security systems and create a cost-effective cyber risk mitigation strategy across their assets. It was a great achievement from ABS's side to show this interesting tool, from ABS expert team's "discovery".

Also, ABS has shown to the maritime industry the wide-range professional and serious services required by addressing the cyber security problem. Their Cyber Security services are divided into: ABS Cyber Security Assessment, Cyber Security Awareness Training, OT Cyber Management Office, Controls System Documents, OT Cyber Incident Response, Management of Change, and Program Standup.

On the 29th of January 2019, in the Smart4sea magazine awards, the ABS received the SMART4SEA Cyber Security Award. Also, in 7th of May 2019, in the second Seatrade Awards, the ABS received the 2019 Seatrade Cyber Security Award for ABS FCI Cyber Risk™ Methodology.
It is important to mention that in March 2019, ABS has announced its partnership with SecurityGate to update and support the ABS FCI Cyber Risk™ Methodology into the SecurityGate SaaS platform, in full. This move showed us how important their tool (FCI Cyber Risk™ equation) is and how they want to up to date.

Additionally, the SecurityGate software helps pinpoint unique remediation efforts to effectively showcase the return on investment of cyber risk mitigation strategies, over time (The Maritime Executive, 2019).

Because of that cooperation as ABS stated: "ABS is a maritime classification society that wants and accepts cooperation with other organizations or companies for the best common interest with partnerships as we see above". Another example was the cooperation with Hyundai Heavy Industries (HHI) to develop cyber security requirements

for the ABS Cyber Security-Ready (CS-Ready) Notation for marine assets (ABS, 2018). Also, Fleet Management Limited signed an agreement with ABS to implement the ABS industry-leading cyber security solution for Fleet Management's 220-vessel liquid cargo fleet (ABS, 2019).

Furthermore, ABS provides on-line seminars in the Cyber Security issue with few of the topics being: Cyber Security for ISPS facilities, effective implementation of cyber security for ports and terminals, and for U.S ports, etc. with a wide range of information for each topic to assist and protect every client, regarding the worth for discussion and reflection issue.

5. CYBER SEAWORTHINESS

5.1 SEAWORTHINESS

After a cyber-attack onboard a vessel, the issue of seaworthiness will be the first that will be examined. So, we have to know everything regarding our vessel's conditions and warranties, under the agreed contract.

Before fixing a vessel or before insurance can be taken out, there is an implied warranty of seaworthiness of the vessel. The term "seaworthiness" is usually conceived in a broad sense. Because the meaning of seaworthiness cannot be explained or defined in a simple way or in one-side path, the essential standard of seaworthiness depends not only upon physical fit, but also on the nature and age of the ship, the type of the carried cargo, the manner of voyage envisaged, and all other relative conditions.

For all these years and in many cases, there was an effort to define the notion of seaworthiness through the courts. But every case had different findings, as the term "seaworthiness" is something so mutable, flexible and versatile. For example, the Nigerian Supreme court defined this term through a case (Narumal & Sons Nigeria Ltd v Niger Benue Transport Company Ltd (1988) 2 NWLR (Pt 106) 730) as: "Seaworthiness for our purpose relates to the suitability of the ship in terms of crew, equipment *(and even carrying the particulars cargo) for the journey being undertaken...*".

The importance of seaworthiness is high and has three main aspects, the technical seaworthiness, fitness for the intended voyage and the “cargo worthiness”. For instance, if a vessel is unseaworthy, there are a lot of risks that arise, like the navigational risk, the environmental risk, the cargo’s risk, the risk for human life, etc. In legal terms, a seaworthy ship is a ship that is, in all respects, fitted for a safe voyage at sea, including the condition of the vessel itself, as well as any equipment on board and the skills and the crew skills (Federico Franchina, 2017). In addition, a ship owner has to consider if his/her vessel is seaworthy, depending on the international standards that are established by the class of the vessel, the vessel’s flag, the departure port, the destination port, the type of cargo, vessel’s equipment, etc.

According to common law, the duty to provide a seaworthy ship on presentation was absolute, i.e. no exceptions were allowed. However, most modern charter party forms have reduced the absolute obligation to a duty of “exercising due diligence”, i.e. doing everything which a prudent ship owner can reasonably do to make the vessel seaworthy without actually guaranteeing her seaworthiness (Generalcargoship.com).

It was enacted at the UAE Maritime Law, Article 227 under Section 2 of Chartering the Vessel for a Voyage, which provides: “The disponent owner must put the vessel in question at the disposal of the charterer, at the time and place agreed, in a seaworthy condition and properly equipped, in such a manner as to carry out the voyage or voyages specified in the charter-party and likewise he must keep the vessel in such condition throughout the voyage or voyages the subject of the charter party”.

Also, the Article 245 Section 3 “Time Charter” and Article 253 section 4 “Bareboat Charter” of the said law, was drafted with the same wording of the aforesaid article.

However, the duty to provide a seaworthy vessel was lessened for the carrier, to only provide a seaworthy vessel before and at the commencement of each voyage, as per Article 272 (1) of the said law which provides that: “1. The carrier must before setting sail and upon the commencement of a voyage use the necessary care to put the vessel in a seaworthy condition and to fit it out, man it and provision it properly. He must prepare the holds and cold rooms and other parts of the vessel to receive, carry and preserve the goods”. (Saif Almobideen, 2012)

5.1.1 CLAUSES FOR SEAWORTHINESS AND SEAWORTHY

Every maritime contract and the clauses included have to be drafted for the sake of interest. The clauses are the biggest tool for of every negotiator before and after a potential incident. So, in here below, there are some examples of the most well-known and important clauses in every maritime contract.

According to Marine Insurance Act 1906 section 39(4): 'A ship is deemed to be seaworthy when she is reasonably fit in all respects to encounter the ordinary perils of the seas of the adventure insured'.

Article III of The Hague/Hague-Visby Rules which incorporate with a paramount clause: "1. The carrier shall be bound before and at the beginning of the voyage to exercise due diligence to: (a) Make the ship seaworthy; (b) Properly man, equip and supply the ship".

Article IV also of The Hague/Hague-Visby Rules: "Neither the carrier nor the ship shall be liable for loss or damage arising or resulting from unseaworthiness unless caused by want of due diligence on the part of the carrier to make the ship seaworthy and to secure that the ship is properly manned, equipped and supplied."

BPVOY4 Condition of vessel Clause: "Owners shall, before, at the commencement of, and throughout the voyage carried out hereunder, exercise due diligence to make and maintain the Vessel, her tanks, pumps, valves and pipelines tight, staunch, strong, in good order and condition, in every way ft for the voyage and ft to carry the cargo (…)."

NYPE 93, Clause 6 (Owner to Provide): "Owners shall provide and pay for the insurance of the Vessel, except as otherwise provided, and for all provisions, cabin, decks,(…), shall maintain the Vessel's class and keep her in a thoroughly efficient state in hull, machinery and equipment for and during the service, and have a full complement of officers and crew."

Other Seaworthiness Clauses: **"**Owners represent and warrant that at all times, during the term of this charter, they shall exercise due diligence to maintain the Vessel in a seaworthy and cargo worthy condition in all respects." Or "Owners shall, before and at

the beginning of each voyage, exercise due diligence to make each Vessel seaworthy, properly manned, equipped and supplied for the voyage, (…)"

ASBATANKVOY Clause 1: "…and being seaworthy and having all pipes, pumps and heater coils in good working order, and being in every respect fitted for the voyage…"

BPTIME Clause 2.1: "Upon delivery the vessel shall be tight, staunch and strong and in every way fit for service…"

5.1.2 SEAWORTHINESS – CASE LAW

According to the English law that is in the most of the times, the law that is applicable to every maritime case, there are many cases that explain why the issue of seaworthiness has so many meanings and approaches. There are several cases that have been represented by the courts, regarding seaworthiness all those years and they have been "made the situation easier" to every lawyer, arbitrator, etc.

Kopitoff v Wilson, [(1876) 1 QBD 602]: "The shipowner is, by nature of the contract, impliedly and necessarily held to warrant that the ship is good, and is in a condition to perform the voyage then about to be undertaken, or, in ordinary language, is seaworthy, that is, fit to meet and undergo the perils of the sea and other incidental risks to which she must necessarily be exposed in the course of the voyage."

Channell J in McFadden v Blue Star Line, [(1905) 1 KB 697]: "A vessel must have that degree of fitness which an ordinary careful and prudent owner would require his vessel to have at the commencement of her voyage having regard to all the probable circumstances of it…Would a prudent owner have required that it (i.e. the defect) should be made good before sending his ship to sea, had he known of it? If he would, the ship was not seaworthy…"

Smith, Hogg & Co V. Black Sea & Baltic (1940) AC 997: "A shipowner was held liable to a charterer in damages for loss of a cargo which had been caused by a combination of perils of the sea and the unseaworthiness of the ship. The latter was sufficient to carry a claim for damages."

Other cases regarding seaworthiness and unseaworthiness:

FC Bradley & Sons vs. Federal Steam Navigation Co. (1926) 24 Ll. Rep 446

The Eurasian Dream (2002) EWHC 118

The Marion (1984) AC 325

CMA CGM Libra (2019) EWHC 481

The Silver Constellation (2008) EWHC 1904

Mitchell v. Trawler Racer, Inc., 362 U.S. 539, 549-50 (1960)

Gebhard v. S.S. Hawaiian Legislator, 425 F.2d 1303, 1310 (9th Cir. 1970)

Cf. Miles v. Apex Marine Corp. , 498 U.S. 19, 32-33 (1990)

14 J. Mar. L. & Com. 69 (1983)

Minister of Food v Reardon Line (1951) 2 Ll. Rep 265

5.2 OFF HIRE AND CLAUSES

There is a possibility, a cyber-attack onboard to occur during an off-hire period. We have to know and be prepared on the off-hire issue and how we can be protected by the maritime contract.

Time charters always set out the defined period, within which a charterer can exploit the commercial operations of the ship and the rate of hire payable to the owner. The risk of any delay is therefore borne by the charterer who, in the absence of any express term, must continue paying hire as agreed. Therefore, most of the time charters therefore contain an off-hire clause, in one wording or another, to clearly state when a charterer is under no obligation to pay the agreed rate of hire (Standard Club, 2018).

Types of Off-hire Clauses fall into two main categories:

1. **‘**net loss of time**’ and**
2. **‘**period**’.**

1. NYPE 1946 CL.15: “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, dry-docking for the purpose of examination or painting of bottom, or by any other cause preventing the full working of the vessel, the payment of hire shall cease for the time thereby lost.”

When the words “any other cause” follow after a list of specific causes in an off-hire clause, there are construed ejusdem generis (to be of similar genus) to the list of causes appearing beforehand.

In Clause 36, inserted in a potential addendum, it is stated: “In the event of loss of time due to boycott of the vessel by shore labour or arising from government restrictions by reason of the vessel’s flag or the terms and conditions on which members of the crew are employed, the payment of hire shall cease for the time thereby lost.”

Although arrests and seizures can fall within the scope of clause 15, these situations might be specifically dealt by an additional off-hire clause in the charter party. For example, the NYPE 1993 form, deals with detention by arrest specifically in clause 17: ‘In the event of loss of time from…detention by the arrest of the Vessel, (unless such arrest is caused by events for which the Charterers, their servants, agents or subcontractors are responsible)…’ This is in line with the implied indemnity principle which acknowledges that a charterer must reimburse an owner for any loss, if the cause of that loss is due to a fault of their own (Standard Club, 2018).

In order to trigger the NYPE clause of the off hire, there are three main and necessary conditions:

i. There must be a loss of time to the Charterers, which
ii. Is caused by an event which falls within the named causes and which
iii. Has the effect of preventing the full working of the vessel (John Wayle).

According to the case of Cosco Bulk Carrier Co Ltd v. Team-up Owning Co Ltd – the M/V Saldanha (2010) EWHC 1340, where the chartered vessel was on the Somali Pirates’ hands for the duration of 63 days. The charterers argued that the vessel should be

off hire during that period of the 63 days. It was proved that the event of “seizure pirates” is an extraneous cause and the charterers cannot benefit from the sweep-up provision.

In a similar way, a hijacking or a cyber-attack is an extraneous cause and the sweep-up provision would not help charterers, if a generic off-hire clause was to be incorporated into the contract.

2. In Clause 21 of Shelltime 3 and 4, is stating that: “the vessel shall be off-hire from the commencement of such loss of time until she is again ready and in an efficient state to resume her service.”, so is a prime example of a ‘period of inefficiency’ clause, which is clearly charterer-friendly in addition to the first category and the NYPE clause which is exactly the opposite and the clause is pro-owner as only the resulting net loss of time is counted as off-hire (Steamship Mutual, 2014).

Summing up, most of the standard Charter Parties are not able to face and allocate every risk arising after a cyber-attack between all parties and Tailor made clauses have to be considered and incorporated into charter parties to deal with the legal issues that emerge, when the chartered vessel is affected from a potential cyber-attack.

5.3 CYBER RISK AND SEAWORTHINESS

As expected, seaworthiness is a concept that includes many areas not only related to maritime law, but also all risks that affect shipping, in general. Usually, we consider seaworthiness as a paradigm of traditional risks affecting shipping during a large period of time, like defects in the hull or structural failure or incompetence and negligence on the part of the crew etc., but in recent decades, while the computer controls have been integrated into the business and operational processes across industries, including the shipping industry, providing relevant results in terms of safety cyber risk is an aspect that sea transport is compelled to keep in high regard by virtue of the almost total informatization of communications and maritime operations. The role of the crew seems to be more and more limited to supervisory tasks. The connection between seaworthiness and cyber risk needs to be interpreted in a broader sense than only focusing on the concept of seaworthiness itself, because a fault of duty may arise within, a shipping

company, resulting in vessel causing delays, business disruption and contractual claims. These considerations may then provide an approach that makes an old warranty fit for new duty (Guireta, 2017).

Nevertheless, there are drafts of off hire clauses dealing with the issue of Cyber Event as stated the below: " In the event of the 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, dry-docking for the purpose of examination or painting of the bottom, Cyber Event, or by any other causes presenting the full working of the vessel, the payment of hire shall cease for the time thereby lost."

"Cyber Event" means any third party act, affecting, the vessel's on-board computers, computer systems or computer software through or by the use of code, computer virus, process or any other electronic means whatsoever, without the consent of the owners.

In fact, many problems arise as a result of nasty accidents caused by hacker attacks against information systems. In such cases, the damaged party could litigate a case of negligence on the part of the ship owner (Guireta, 2017).

Moreover, failing to protect the vessel against a cyber event could be a failure to exercise due diligence to make the vessel seaworthy. This may also be a breach of Articles 3(1) and 4(1) of the Hague/Hague-Visby Rules and could lead to a claim under a bill of lading (HFW).

5.4 INTERRUPTION TO LAYTIME AND DEMURRAGE

As the concern of an off-hire issue for the time charter contracts emerges, it is also the concerning of a demurrage issue to voyage charter contracts. One of the risks in a voyage charter party is the delay that arises from loading and/or discharging operations.

Laytime and demurrage runs continuously and without any interruption, unless an exceptions clause applies or there is a delay, caused by the owner. Most common laytime exception clauses are narrow in their construction and only relate to the vessel itself. Such an exception clause may well respond to a cyber event which affects the vessel

directly, but will probably not include a situation where it is the port or terminal that is suffering from a cyber event (HFW, 2016).

5.5 CAUSATION

Unseaworthiness gives rise to civil liability only if it actually causes loss or damage, and / or addressed in the charter party, pursuant to Article 228 of the UAE Maritime Law.

Causation is simply codified in Marine Insurance Act section 55(1): 'Subject to the provisions of this Act, and unless the policy otherwise provides, the insurer is liable for any loss proximately caused by a peril insured against, but, subject as aforesaid, he is not liable for any loss which is not proximately caused by a peril insured against.

Although, in Article 228 of the UAE Maritime Law provides expressly that: "The lessor shall be liable for any damages arising to the goods received by the master on board the vessel within the provisions of the charter-party, unless it is established that the lessor fulfilled his duties referred to in the preceding and the damage did not arise from his default."

5.6 THE BURDEN OF PROOF

In every law case, there is always a question that has to be answered and in many occasions, has a different point of view, depending on the cases and the facts. Whether the current position of law on seaworthiness should be maintained, taking into account developments in the shipping industry and in particular: the time at which the vessel should be seaworthy, basis of liability of the carrier and burden of proof remains to be seen.

The burden of proving unseaworthiness/seaworthiness should be shifted towards to the carrier, and should be exercised before seeking the protections of the law or carriage contract.

According to the provisions of paragraph 1 of Article III of the Hague/Hague-Visby Rules, whenever loss or damage has resulted from unseaworthiness the burden of proving

the exercise of due diligence shall be on the carrier or other person claiming exemption under this article."

5.7 CONCLUSION

One question that must be asked and is yet to be answered by the Courts is whether the threat of Cyber-attacks can be described as an ordinary peril of the seas. Before answering this question, it should be mentioned that, ordinarily, the perils of the seas are understood to be the ordinary actions of the winds and waves.

On the other hand, for a vessel to be seaworthy, its master and crew must be competent to man the vessel .i.e. they must be familiar with all of the procedures to follow operate the vessel in a manner (Medani, 2017). There is another principal that every company has to face and protect by preparing and training their employees and seafarers from their internal procedures systems. (See on the chapters below)

6. BIMCO, CHARTER PARTIES AND CONTRACTS

6.1 INTRODUCTION

After the publication and issuance of the "the Guidelines on Cyber Security Onboard Ships", BIMCO had the mission to create a new contractual Clause, the BIMCO Cyber Security Clause in order to protect and minimize the risks from all sides that are involved in a contract. BIMCO's Documentary Committee had agreed for drafting a new standard Clause. On May 2019, a drafting team with head Ms. Inga Frøysa of Klaveness, Oslo, and representatives from ship owners, P&I clubs and a law firm (Navig8, UK P&I Club, and HFW), published the BIMCO Cyber Security Clause which is written in generic and broad language, to facilitate every member and everyone to read it and use it to any contract and in a string of contracts for easy back-to-back application. "I am very pleased to see BIMCO as the first mover on this important topic. Recent years have shown that

there is a clear need for a clause addressing the contractual issues that can arise from a cyber security incident," says Inga Frøysa.

6.2 THE BIMCO CYBER SECURITY CLAUSE

In this part of the research, we have to see and analyze the BIMCO Cyber Security Clause, as it is, and how it suits every contract:

(a) Each Party shall:

(i) Implement appropriate Cyber Security measures and systems and otherwise use reasonable endeavors to maintain its Cyber Security;

(ii) Have in place appropriate plans and procedures to allow it to respond efficiently and effectively to a Cyber Security Incident; and

(iii) Regularly review its Cyber Security arrangements to verify its application in practice and maintain and keep records evidencing the same.

(b) Each Party shall use reasonable endeavors to ensure that any third party providing services on its behalf in connection with this Contract complies with the terms of subclause (a)(i)-(iii).

(c) If a Party becomes aware of a Cyber Security Incident which affects or is likely to affect either Party's Cyber Security, it shall promptly notify the other Party.

(i) If the Cyber Security Incident is within the Digital Environment of one of the Parties, that Party shall:

(1) Promptly take all steps reasonably necessary to mitigate and/or resolve the Cyber Security Incident; and

(2) as soon as reasonably practicable, but no later than 12 hours after the original notification, provide the other Party with details of how it may be contacted and any

information it may have which may assist the other Party in mitigating and/or preventing any effects of the Cyber Security Incident.

(ii) Each Party shall share with the other Party any information that subsequently becomes available to it which may assist the other Party in mitigating and/or preventing any effects of the Cyber Security Incident.

(d) Each Party's liability for a breach or series of breaches of this Clause shall never exceed a total of USD _____ (or if left blank, USD 100,000), unless same is proved to have resulted solely from the gross negligence or willful misconduct of such Party.

Subclause (a)

The first subclause explains that every party has to take their cyber security measures to be cyber security reliable. Every company has to establish or should have already established specific systems according to the company's size, location and day to day communications. The word "appropriate" is used for this reason here but also the parties that are involved here must maintain all their cyber security measures and systems and not only to implement them. Moreover, the parties have to be able to understand and update every necessary measure, depending on the various threats that this world faces every day, the "appropriate" procedures.

Subclause (b)

The second subclause states that every party has to use reasonable endeavors to secure that any third party operates with secure systems and they never cause any harm through any non "appropriate" cyber security system. As a result, it complies with the subclause (a). For example a shipbroker communicates with both sides, under the agreement with the ship owner and the charterer or with agents and the managers, via emails or other digital systems, and they have to be as careful as the other parties.

Subclause (c)

The third subclause has more complex review. Firstly, the party who becomes aware of a cyber security incident has to warn the other party, but this obligation does not only apply on the other party's systems, but also on every incident that comes around the sector's world.

Also, the systems of the other party must detect anything or their professionals must be curious on anything "different" than normal from the other side system. Secondly, in the subclause (c)(i)(2), the party that seems to be affected, is obligated to report the current condition in a specific time limit that the subclause states (12hours), from the time that they detect the incident and provide them alternative ways of communication, without risking their systems too. In addition to, this in the subclause (c)(i)(1) the party has to take action immediately to resolve every problem presented by an incident in its "Digital Environment". The wording of "The action to be taken must be reasonably necessary" was chosen so as to reflect that a party cannot be expected to take measures that are, e.g., too costly, compared to the extent of the incident. The subclause (c)(ii) states that every party has to provide and help with relevant information, regarding the incident, to facilitate the other party.

Subclause (d)

The last subclause has the limitation of liability and provides a blank space to be filled out with the liability cap, with a default limitation on the amount of USD 100,000.00 that will be applied if the parties do not to cover an amount. The reason behind this subclause is that, maritime cyber security insurance is in premature stage and, for now, there is no obligation for the parties to have a premium for this case, some insurance companies are not cover losses from a cyber-attack and some have specific conditions. So, this subclause will be helpful for these parties trying to purchase an insurance based on the limitation of USD 100,000.00.

The aim of drafting this clause was to aware all the ship owners, managers, charterers and agents of the fact that a cyber-attack is a possible scenario for everyone without any exceptions, nowadays. The other one is to encourage every party of the contract to have or create plans and procedures, in order to minimize the possibility of every cyber threat

and risk of a possible incident by increasing the readiness of every party and their employees and also to minimize the effects of such an accident.

In the early stages of development, the drafting team discussed if the clause should also address payment fraud. They concluded that the risk of this increasingly common fraud is probably best dealt with at a procedural level by companies tightening up their internal payment procedures and require verification of any changes to payment details (Mads Wacher Kjaergaard, 2018).

BIMCO uses tight wording with the phrase “appropriate” cyber security to ensure that every party of a contract is safe and no one will cause harmful side effects to the other party during a potential cyber incident and during the contract, in general. Just like the “the Guidelines on Cyber Security Onboard Ships” of BIMCO, the BIMCO Cyber Security Clause will be established in a lot of contracts and a lot of maritime organizations will encourage BIMCO’s effort to understand the serious issue of the maritime cyber security offshore and ashore and every risks, threats and their effects on every company in the industry. As it is understandable, the shipping industry becomes more aware and sees on the risks of cyber-attacks. Mr. Itai Sela, the CEO of the Israel-based Naval Dome releases a statement in Tanker Shipping and Trade Conference & Awards in London, saying the timing of the BIMCO cyber clause, set to precede by nearly two years the 2021 IMO, a mandated deadline for cyber security concerns to be added to the ISM Code, meant ship owners were taking cyber security seriously.

6.3 ELECTRONIC BILL OF LADING

The global maritime trade in goods involves many parties every day, including carriers, distributors, cargo interests, banks, insurers, government agencies, terminals and customs authorities. As a result, a lot of documents need to be generated, copied and sent all over the world, in papers form. So, according to the Information and Communications Technology (ICT), some of the above parties were quick to take advantage of Electronic Database Interchange (EDI) systems capable of transferring data from computer to computer to speed up their transactions in their trades. For example, documents such as

invoices, booking notes, booking confirmation slips and even sea waybills, became routinely generated and transmitted electronically.

There are currently three electronic Bills of Lading systems in the market, approved for use by the International Group of P&I Clubs: BOLERO (the oldest of the three), ESS and E-Title (the newest entrant). In addition, there are other new challengers in the market who are developing new systems relying on distributed ledger technology. Those three types of eB/Ls require all users to sign up to a multi-party contract in order for their electronic systems to replicate, the law by contract, behind paper bills of lading (Norton Rose Fulbright, 2018).

6.3.1 CHALLENGES BETWEEN A PAPER BILL OF LADING TO AN ELECTRONIC BILL OF LADING

However, there was some attempts to create an eB/L that faced more challenges because there are a lot of delays on a "traditional" bill of lading in paper. Firstly, most of the times, a vessel arrives at the destination port before the paper bill of lading that is transported via courier. So, this means that the delivery of cargo has to be delayed, but as the port traffic is huge every day, no one can wait for another vessel. As a result, a demurrage claim or extra costs for receivers and charterers to store their product, are the most common solution. Instead of requiring numerous originals and copies that take several days to process, only one electronic document is securely produced and processed through the system, eliminating document delays as well as the potential for fraud (BIMCO, 2016).

Another problem of paper B/Ls is the fact of secureness. A bill of lading is a document of title and every person who has this document is the owner of the cargo but is a transferable document too. But paper BLs can easily be forged, stolen or lost and, most of the times, the carrier to avoid any delays, agrees to deliver any of the cargo with the LOI or a Bank guarantee from the receiver's side. However, the carrier remains responsible for the misdelivery claims, under forged or stolen BLs. Fraud is a real risk because paper bills can be forged or switched. As a matter of English law, delivery against a forged bill

of lading is a misdelivery. The argument that it was done innocently cannot withstand (Norton Rose Fulbright, 2018).

Last but not least, the cost of issuing an electronic bill of lading differs from a paper bill of lading. This costs are estimated to be approx. of 15% of the physical transportation costs. When eBLs are used, the requirement for LOIs is reduced by some 90%.This means a huge reduction in costs for the participants involved (UK P&I Club, 2017).

In 1990, the Comité Maritime International (CMI) published its 'Rules for Electronic Bills of Lading, which provided an elaborate complex system for overcoming the problem of proving title to goods by electronic means. The swiftness with which transactions could be completed, through electronic medium, led to its universal acceptance compelling the Indian Parliament to take note of the same and enact a law facilitating electronic commerce (ICC, 2018).

At present, there are no international cargo conventions in force that apply to e-Bills, so parties will have to incorporate the various rules by contract if they want them to apply. The Rotterdam Rules, although not yet in force, provide for the equal value of transport documents and their electronic equivalent, the electronic transport record (Nielsen, 2016).

Moreover, to achieve and protect all parties' sides, BIMCO has drafted the BIMCO Electronic Bill of Lading Clause by a committee, consisting of representatives from owners, charterers and the International Group for use in charter parties. So, the BIMCO's for eBLs' clause needs to be incorporated into charter parties if the parties intend that charterers will have the right to order owners to issue eBLs (UK P&I Club, 2017).

On the other hand, the current concern for the eBLs is the cyber risks that arise on this area too. Although there have been several cases and case precedents, involving electronic documents, we are not aware of any past or current cargo claims or disputes involving eBLs. essDOCS, Bolero and e-titleTM have also confirmed that they are not aware of any cases in any jurisdiction questioning the validity of an eBL. All the three systems approved by the Clubs already use cryptography and encryption to address the problem of security (UK P&I Club, 2017).

6.3.2 THE BIMCO ELECTRONIC BILLS OF LADING CLAUSE 2014

It is common knowledge the maritime companies are divided into two different parts. There are the “traditional” ones and the modern shipping companies that are nowadays suggest the two different types of Bills of Lading. The main concerning is the cyber security issue that is involved in this decision too.

Regarding the stress on the electronic Bills of Lading, BIMCO has drafted the Clause below:

(a) At the Charterers’ option, bills of lading, waybills and delivery orders referred to in this Charter Party shall be issued, signed and transmitted in electronic form with the same effect as their paper equivalent.

(b) For the purpose of Sub-clause (a) the Owners shall subscribe to and use Electronic (Paperless) Trading Systems as directed by the Charterers, provided such systems are approved by the International Group of P&I Clubs. Any fees incurred in subscribing to or for using such systems shall be for the Charterers’ account.

(c) The Charterers agree to hold the Owners harmless in respect of any additional liability arising from the use of the systems referred to in Sub-clause (b), to the extent that such liability does not arise from Owners’ negligence.

Under sub-clause (a) of the BIMCO clause, owners and charterers agree that the eB/L issued will have the same effect as a paper BL.

7. MARITIME INFORMATION SYSTEMS IN RELATION TO CYBER SECURITY AND CYBER-ATTACKS

7.1 INTRODUCTION

Traditionally, attacks focused on marine vessels including piracy, boarding, theft, and/or destruction. These attacks were often successful, as it is difficult to call and receive help quickly while travelling across the sea. While these threats continue, they are now well understood and there are centuries of experience in mitigation actions. On the contrary, today's cyber-attacks are much more stealthy and often kept “under the radar”, in order to exploit the compromised vessel for a longer period of time and, hence, for greater profit. Current threat implications of marine-based cyber-attacks include business disruption, financial loss, damage to reputation, damage to goods and environment, incident response cost, and fines and/or legal issues (Tam, Papadakis, Jones, 2012).

Nowadays, the issue of Cyber Security concerns and attacks the attention of all in the maritime sector. On the other hand, cyber-attacks keep repeating on different targets every time due to lack of investments in Cyber Security. There are a lot of ship owners that are not convinced on this major problem that can happen to anybody on the shipping industry. Every annual report, from maritime organizations, companies, classification societies, etc. show us that cyber-attacks are increased every year within a big percentage, which is explained by digitalization and the need of new technologies and electronic data that are uploaded every day in every company’s information systems, both offshore and onboard.

The more obvious and one of the first targets of a cyber-attack are divided in two different areas. The attack surface could basically be a cyber threat to vessels and a cyber threat offshore. The best way to face and then to solve such as issue is to analyze every possibility, gaps and vulnerabilities that we have on this two areas.

7.2 MARITIME MONITORING SYSTEMS

As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are increasingly being networked together and more frequently connected to the internet.

The need of carrying a variety of goods and services are nowadays in high levels. Shipyards provide their high quality services to every ship owner in the maritime industry, who wants a ship, within a specific time frame, and as a result they compete each other for their technology and systems that could be provided.

Information technology systems are those focusing on the use of data as information. Operational technology systems, on the other hand, focus on the use of data to control or monitor physical processes. For example, sensor data or GPS data.

The main ship types are:

- the container vessels,
- the bulk carriers,
- the tanker vessels,
- the cruise and ferry ships,
- the fishing vessels
- the oceanographic and meteorological ships,
- the tug boats,
- the icebreakers,
- the army's vessels,
- the search and rescue vessels, etc.

Every vessel has mandatory specifications to fulfill for i.e. size, equipment, number of crew, information and monitoring systems, etc.

Maritime Monitoring systems can divided to:

- Reporting systems
    - COSPAS-SARSAT
    - Inmarsat

    - Global Maritime Distress and Safety System (GMDSS)
    - Automatic Identification System (AIS)
    - Long-Range Identification and Tracking system (LRIT)
    - Vessel Monitoring System (VMS)
- Observation systems
- Hybrid Systems

Scenario:

In the modern maritime history, there were many accidents recorded, with terrible causes from bad weather conditions, or dangerous cargo that a vessel was carry, by human mistakes, by technical malfunctions that caused a breakdown in the main engine of the vessel, by terrorism or piracy where the vessel passed from high risk areas like the Indian ocean, etc.

What if the Exxon Valdez's accident, in 1989, wasn't a simple accident like others but it was a cyber-attacks that caused a terrible environmental issue to the Alaskan waters and a financial and reputational issue to Exxon Mobil?

What if the Costa Concordia's accidents, in 2012, wasn't a simple accident caused by the captain of this cruise ship but it was a cyber-attack that caused the lives of many people?

If we face all these terrible accidents as cyber-attacks' accidents, we can understand the importance of the maritime cyber security. Unfortunately, few of us can see the concerns that arise and their solutions too.

The maritime industry has already faced Cyber-attacks, causing big financial and commercial losses. But there are not many reports for cyber-attacks on vessels' monitoring systems. But, some companies have already presented some potential cyber-attacks to help ship owners suspect the problem and the corresponding situation. Some of them are:

- Hacking of Electronic Chart Display and Information System (ECDIS) demonstrated by NCC Group.

- Hacking of Automatic Identification System (AIS) demonstrated by cybersecurity firm Trend Micro.
- Jamming of GPS demonstrated by the UK and Irish General Lighthouse Authority.
- Hacking of Global Positioning System (GPS) demonstrated by researchers at University of Texas at Austin.

7.2.1 COSPAS-SARSAT SYSTEM

COSPAS-SARSAT is a system designed to detect and support emergency beacons, activated by aircraft, ships and people engaged in recreational activities in remote areas, and then sends these distress alerts to search and rescue (SAR) operations authorities, with the main purpose of the detention of distress alerts, caused by personal use or by the maritime domain, or by the aviation domain. From 1988 to 2017, the Cospas - Sarsat System has provided assistance in approximately 13,000 SAR events, with a major percentage in maritime events (50%). It seems throughout these years, up to now, that their statistics have gradually increasing regarding the SAR events.

Certainly, the basic Cospas - Sarsat System for maritime purpose is composed by:

- The EPIRB: the Emergency Position-Indicating Radio Beacon which is used to alert search and rescue services in the event of an emergency, some of them include a GPS receiver. Generally, EPIRBs differ each other and they have categories. For example, the category I EPIRB is activated manually or automatically when a vessel is sinking, but the II EPIRB can only be activated manually;
- Instruments on board satellites in geostationary and low-altitude Earth orbits which detect the signals transmitted by distress radio beacons;
- Satellite ground stations, referred to as Local Users Terminals (LUTs), which can receive emergency beacon distress alerts. Also, LUTs have two types the LEOLUTs which are designed to operate with the LEOSAR satellites and the GEOLUTs which are for the GEOSAR satellites;

- Mission Control Centers (MCCs) which can collect, store and sort the data received by LUTs, provide data exchange within the Cospas - Sarsat System and forward them to Rescue Coordination Centers (RCCs), Search and Rescue Points Of Contacts (SPOCs) or other MCCs.

The Cospas - Sarsat System includes three types of satellites:

- The LEOSAR system, satellites in low-altitude Earth orbit (LEO). They have limited coverage of the earth, while there may be one hour between the transmission and the reception of a distress signal, which five satellites are orbiting above the poles (850km-1.000km). They can also determine the position of EPIRBs with an accuracy of 2-5 km.
- The GEOSAR system, satellites in geostationary Earth orbit (GEO), which six satellites are orbiting over the equator (36.000 km). They cover most of the area of the Earth (with the exception of the poles) and they can emit instantly distress signals, but they cannot determine the position of an EPIRB.
- The MEOSAR system, satellites in the medium-altitude Earth orbit (MEO). The MEOSAR system is the future of the Cospas - Sarsat system. This system combines the advantages of LEOSAR and GEOSAR systems together. Recently, they have been added and orbiting between 2.000 and 36.000 km. There are over thirty MEOSAR in service and it is expected that over seventy satellite will be in use, in the next years.

In a typical COSPAS-SARSAT search and rescue scenario, the following steps take place:

STEP 1: DISTRESS SIGNAL ACTIVATION

STEP 2: SATELLITE COMMUNICATIONS

STEP 3: GROUND STATION RELAY

STEP 4: MISSION CONTROL CENTER COORDINATION

STEP 5: RESCUE COORDINATION CENTER COORDINATION

STEP 6: (MEOSAR ONLY) RETURN LINK SERVICE

Source: website of COSPAS-SARSAT.in

7.2.2 INMARSAT

Inmarsat plc is a British satellite telecommunications company, with headquarters in London, which was founded in 1979, offering global mobile services, by owning and operating a global satellite network. It provides telephone and data services to users worldwide, via portable or mobile terminals which communicate with ground stations through thirteen geostationary telecommunications satellites (Inmarsat, 2019). The main uses of this network are:

- The fleet management
- The fishing control
- The transfer of (confidential) data
- The security Services (i.e. GMDSS, EPIRB, SART, DSC, NAVTEX).
- The maritime monitoring for environmental protection.

Inmarsat's systems are mainly divided in two different areas:

- Satellite system: there are four satellites in service, covering most of the areas on earth (excluding the poles), the satellite coverage includes 4 overlapping areas: the Atlantic Ocean-East (AOR-E), the Atlantic Ocean-West (AOR-W), the Pacific Ocean (POR) and Indian Ocean (IOR).
- Terrestrial Network: is a network consisting of Land earth Stations (LES), Mobile Earth Stations (MES), Network Co-ordination Stations (NCSs) and a Network Operations Centre (NOC).

7.2.3 GLOBAL MARITME DISTRESS AND SAFETY SYSTEM (GMDSS)

The GMDSS has been developed for vessels above 300 gross tonnage (GT) in order to support safe shipping. Moreover, with the use of GMDSS a vessel in distress can alert instantly rescue centers as well as nearby ships.

The main components of GMDSS are:

- The Inmarsat
- The EPIRB
- The Search and Rescue Locating Equipment (SART): these systems are compatible with EPIRB but they are not designed for the transmission of distress signals. However, ships within the range of eight nautical miles can locate a SART and therefore to provide help even in low visibility conditions.
- The Digital Service Calling (DSC): it allows the transmission of data such as the id of the ship, its position and the channel for further communication. It automates the process of distress signal transmission with the use of terrestrial channels of communication. Moreover, this signals have a specific format and are transmitted either to shore-based Maritime Rescue Co-ordination Centers (MRCCs) or nearby ships.
- The Navigational Telex (NAVTEX): it is an international automated medium frequency direct-printing service for delivery of navigational and meteorological warnings and forecasts, as well as urgent maritime safety information (MSI) to ships. Moreover, according to the SOLAS Convention, the NAVTEX is a

mandatory element for vessels, depending on vessels' classes, from August 1993. Also, the range of NAVTEX can reach up to 600 nautical miles from the coast and there are 16 areas globally (NAVAREA) and 24 stations in each area.

7.2.4 AUTOMATIC IDENTIFICATION SYSTEM (AIS)

The most popular system in the world and not only in the maritime sector is the AIS system, if we can imagine how many people have already visited the website of marine traffic (www.marinetraffic.com), at least once.

The AIS system was created to improve safe navigation of vessels, prevent collisions and support the port authorities in the management of maritime traffic and with the primary goal to provide information about the location of vessels. In addition, the IMO's International Convention for the Safety of Life at Sea requires AIS to be fitted aboard international voyaging ships with 300 or more gross tonnage and all passenger ships regardless of size.

Nowadays, AIS data are divided in three main categories, the static, the dynamic and the route-based. AIS information is used to serve various purposes and facilitates the work of people in various occupations, such as (among others), (marinetraffic, 2019):

- Port Authorities and Harbor Masters
- Ship Owners, Managers and Builders
- Ship Agents, Brokers and Charterers
- Researchers and Data Analysts
- Tug Operators and Pilots
- Search and Rescue teams
- Flag administrators and Classification Societies
- Vessels' crews and their families' members
- Coast Guard and Border Patrol

- Hotels and Tour operators
- Passengers or recreational sailors
- Environmental Protection agents
- Maritime Enthusiasts and Radio-amateurs, etc.

A typical range of AIS is:

1. Satellites/GPS collect AIS messages;
2. Vessels within 50 km exchange AIS messages;
3. Coastal base stations receive AIS messages;
4. Communication between vessels and base stations using Aid-to-Navigations (AtoN); and
5. Forwarding of AIS messages in Information systems for processing.

7.2.5 LONG-RANGE IDENTIFICATION AND TRACKING SYSTEM (LRIT)

The Long-Range Identification and Tracking (LRIT) system provides global identification and tracking of ships. This system shows the vessel's position, the timestamp of the message, information which is confidential and the transmission of ID, by default every 6 hours with satellite communications using the GMDSS equipment. They are using it in merchant vessels, over than 300 GT, and passenger ships.

The obligations of ships to transmit LRIT information and the rights and obligations of SOLAS Contracting Governments and of Search and rescue services to receive LRIT information are established in regulation V/19-1 of the 1974 SOLAS Convention (IMO).

7.2.6 VESSEL MONITORING SYSTEM (VMS)

The vessel monitoring system (VMS) is a satellite-based monitoring system, which at regular intervals, provides data to the fisheries authorities on the location, course and speed of vessels (European Commission, 2019). The VMS is a system that can

automatically transfer regular data regarding vessels' id, geographical position, and timestamp of the message, vessel's speed and heading (degrees) also by transferring them to the Fisheries Management Agency.

In addition, every fishery has or should have the E-logbook, which can replace the hand-written fish selling logs and the ship's calendar which contained the fish records of the trip and was delivered in time to the appropriate port authorities. In Electronic Reporting System (ERS), the vessel's master registers and sends the daily fishing data, as the name and vessel's ID, the geographical area, the fishing equipment is used, the unloading locations and quantities and the daily sales.

7.3 COMPANY'S TYPICAL PROCEDURES REGARDING CYBER SECURITY

Every company is obliged to draft and issue procedures for the employees and seafarers who are working there and as a result everyone are obligated to know the company's procedures. The main purpose is to be prepared and know everything regarding a problem that will be able to harm their company. There are many issues in every company's procedure guide and one of them is the Cyber Security. In the context below we will see a typical procedure for a company and some examples, regarding the Cyber Security issue.

7.3.1 DATA BACK UP OF OFFICE SERVERS

a. Full back up is conducted every working day by the IT department:

i. For the Accounting Program back up is conducted by the IT Assistant every working day (one tape for each working day of the week).

ii For NS5 and other applications and data, back up is conducted automatically by the available servers.

b. Back up is carried out on each server separately.

c. The back-up tapes of the previous working day are kept in the residence of the IT Manager or the IT Office Assistant for safety reasons.

d. The backup of the telex/fax/E-mail communications through the Telex Computer System is conducted on a daily basis by the Telex Operators, and the back-up tapes of the previous working day are kept in the residence of the Telex operator.

7.3.2 DATA BACK-UP OF COMPANY'S INDIVIDUAL PCS

a. Users, at office and on board the managed vessels, are responsible for backing up their own files, at their will.

b. Backups can be carried out in one or both of the following ways:

i. By copying data to a pre-specified location on a server machine.

ii. By using the backup facilities of the Windows OS to back up data to diskettes.

c. Instructions are given by the IT department on a request basis or whenever it is deemed necessary.

7.3.3 VIRUS PROTECTION / CYBER SECURITY

Cyber security should be considered at all levels of the company, from senior management ashore to onboard personnel, as an inherent part of the safety and security culture necessary for the safe and efficient operation of the ship. The objective is to provide a safe working environment by establishing safe practices and procedures based on an assessment of all identified risks to the ship and personnel by following below steps:

- Identify and Detect a cyber-threat: Define roles and responsibilities for cyber risk management and identify the system, software and operating systems vulnerabilities, data and capabilities that when disrupted pose risks to ship operation and, implement activities necessary to detect a cyber-event in a timely manner.
- Protect against a cyber-attack: Implement risk control processes and measures and develop activities and plans to provide resilience to protect against a cyber-attack and ensure continuity of shipping operations.
- Recover after a cyber-attack: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-attack. In identifying a cyber-threat, equally important that knowing the technology and software vulnerabilities is knowing the substantial threat of human element as shown in table below:

Group	Motivation	Objective
Activists / Dissatisfied employees	Reputational damage Disruption of operations	Destruction of data Publication of sensitive data Media attention Denial of access to the service or system targeted
Opportunists	The challenge	Getting through security defenses Financial gain
Criminals	Financial gain Commercial espionage Industrial espionage	Selling stolen data □ Ransoming stolen data □ Ransoming system operability □ Arranging fraudulent transportation of cargo □ Gathering intelligence for more sophisticated crime, exact cargo location, off vessel transportation and handling plans etc.
States Terrorists	Political gain Espionage	Gaining knowledge Disruption to economies and critical national infrastructure

In general, there are two types of cyber-attacks, which might affect the company and the ships. Untargeted attacks, where the company and ship's system and data are one of many potential targets and the targeted attacks where company is the intended target. Untargeted attacks are likely to use tools and techniques available in the internet which can be used to locate, discover and exploit widespread vulnerabilities which may also exist in the company and onboard a ship, such as:

- **Malware (malicious software):** is designed to access or damage computer without the knowledge of the owner including Trojans, spyware, viruses and worms
- **Social engineering:** a non-technical technique used to manipulate insider individuals into breaking security procedures through interaction via social media
- **Phishing:** emails to a large number of potential targets asking sensitive or confidential information. Such emails may also request to visit a fake website using a hyperlink.
- **Water holing:** establishing a fake website or compromising a genuine one to exploit visitors
- **Scanning:** attacking large portions of the internet at random
- Targeted attacks are more sophisticated using techniques specifically created for targeting the company, such as:
- **Denial of service (DoS):** prevents legitimate and authorized users from accessing information, usually by flooding a network with data. This attack takes control of multiple computers and/or servers.
- **Spear-phishing:** individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software
- **Subverting the supply chain:** attacking the company and/or ships by compromising equipment, software or supporting services being delivered to the company and/or ship

7.3.3.1 RISK ASSESSMENT

The goal of the assessment of a ship's network and its systems and devices is to identify vulnerabilities that could compromise the operation of the equipment, network or even the ship. Risk assessment process has improved safety of the company and ships. Tests of critical system infrastructure have been performed by IT personnel in order to map their robustness to handle the current level of cyber threats. See relevant form Risk Assessment Form.

7.3.3.2 PROCEDURAL CONTROL MEASURES

Protection against threats can be achieved most of the time through simple reflexes. Procedural controls are focused on how personnel use the onboard systems and safety measures are taken, and for the most part should be applied by all its members. Extensive plans and procedures that contain sensitive information should be kept confidential and handled according to company policies, distribution of roles and responsibilities between the ship and headquarters. Procedural actions are segregated as follows.

a) Procedural protection measures for onboard personnel:

i. Use of administrator privileges.

Administrator privileges should only be given to appropriately trained personnel who have a need, as part of their role in the company or on board to log into systems using these privileges. User privileges should be removed when the people concerned are no longer on board. To protect access to confidential data and safety critical systems, a robust password policy is developed.

ii. Careful choice of passwords.

- Passwords should be strong and changed periodically.
- Passwords should not be stored in files or on post-it notes.
- Always locked sessions, even during a short absence, to prevent unauthorized access to workstation.

iii. Password management.

A designated form is used for password management.

- This form is completed by IT vessel operator and handed over only to master.
- If password changes occur and must be updated.
- One hard copy is stored inside IT Dept. and another in vessel’s safe under Master’s custody.
- Records of changes are kept only by IT personnel.

iv. Email and antivirus protection.

Email and attachments play a key role in the most common compute attacks. Opening malicious emails may damage the user's computer and jeopardize the entire information system. Crew personnel should take the following precautions. Check the consistency between the alleged sender and the message content and his sender's identity. Every employee has to be aware of some simple tips for antivirus and threats protection:

- Do not open attachments from unknown senders.
- Never reply by email to a request about personal or confidential information.
- Possible phishing by imitating the look of well-known institutions in order to steal data.
- Disable automatic opening of downloaded documents.
- Email as zip or encrypted file when necessary to headquarters.
- Do not open any files attached to an email from an unknown, suspicious or untrustworthy source.
- Do not open any files attached to an email unless you know what it is, even if it appears to come from a friend or someone you know. Some viruses can replicate themselves and spread through email. When in doubt, call the sender of the email and verify its authenticity.
- Do not open any files attached on an email if the subject line is questionable or unexpected.
- Delete chain emails and junk emails. Do not forward or reply to any of them. These types of email are considered spam – unsolicited, intrusive messages that clog up the inboxes and networks.
- Do not download any files from strangers.
- Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks the files on the download site.
- Update your antivirus software regularly. Various anti-Virus software update automatically and continuously via the Internet.

- Back up your files on a regular basis. If a virus destroys your files, at least you can replace them with your back-up copy. You should store your backup copy in a separate location from your work files, one that is preferably not on your computer.
- When in doubt, do not open, download, or execute any files or email attachments. Not executing is the more important of these caveats.

In order for scanning software tools to detect and deal with malware, they need to be updated. Updates are distributed to ships on a timely basis and that all relevant computers onboard are updated. Furthermore, there is a template with anti-virus tips to ensure proper use of internet by all crew members.

v. Personal use policy

The use of personal devices in a professional context can affect the safety of ship or company data such as data leakage, intrusion, theft or loss of devices etc. Is therefore recommended to separate personal and professional uses.

- Do not forward professional email to personal mailboxes.
- Do not store professional data to personal devices (USB drive, smartphone, etc.) or on personal online storage tools.
- Do not connect personal removable media to the ship's or company's computer.
- Do not connect ship's authorized removable media to personal devices such as laptops.

vi. Responsible use of social media.

Social media is a place where people exchange information, opinions and experiences to learn, develop and have fun. Whether employees are handling a corporate account or use one of their own, they should remain careful and productive. Careless use of social media might arise issues and thus some practical advices are followed:

- Use of common sense.
- Do not neglect job duties to spend time on social media which might lead to declined productivity.

- Avoid sharing intellectual property without approval. Confidentiality laws and policies always apply.
- Avoid any defamatory, offensive or derogatory content.
- Avoid making allegations about others.
- Do not forget to log out of shared machinery.
- Do not share personal pictures or information.

vii. Unauthorized software.

Cyber-attacks aim for software that they can exploit to gain control of and the use to access other devices, accounts and data. If IT Dept is unaware of software running on the network, it is unlikely to maintain proper security updates and configurations, increasing the likelihood of successful attacks and compromises. In this context, several measures shall be taken in order to ensure the security of onboard operating systems, data and the ship.

- Ensure that software, including downloaded software, is properly licensed, free of malicious code, and authorized before installing.
- Abstain from loading unapproved software from unauthorized sources on systems or networks. An unauthorized source is any location (e.g., file store or server to which a device could connect, Internet site, intranet site) or process that is not permitted by IT personnel for distribution of software.
- Log-off or lock systems when leaving them unattended.
- Keep sensitive information out of sight when visitors are present.
- Permit only authorized users to use equipment and/or software.
- Protect information assets from unauthorized access, use, modification, destruction, theft, or disclosure and treat such assets in accordance with any information handling policies.
- Ensure important data is backed up, in particular, on a server that is backed up on a regular basis.
- Secure backups.
- Do not use another person’s account, identity, or password.
- Do not exceed authorized access to sensitive information.

- Do not share sensitive information, except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Do not use sensitive information for anything other than the purpose for which it has been authorized.
- Do not access information for unauthorized purposes.
- Do not use sensitive data for private gain or to misrepresent or any other unauthorized purpose.
- Do not use of iPods, USB sticks, PDAs and other portable storage devices on both office and vessels network. Failure to do so can lead to data theft, introduction of viruses, legal liability issues and more.

b) Procedural protections measures for IT personnel:

i. Training and awareness.

Training and awareness is the key supporting element to an effective approach to cyber safety and security. Applicable personnel both onboard and shore side should know all above mentioned procedures and furthermore the signs when a computer has been compromised. This may include the following:

- An unresponsive or slow to respond system.
- Unexpected password changes or authorized users being locked out of a system.
- Unexpected errors in programs, including failure to run correctly or programs running unexpectedly.
- Unexpected or sudden changes in available disk space or memory.
- Email being returned unexpectedly.
- Frequent system crashes.
- Abnormal hard drive or processor activity.
- Unexpected changes to browser, software or other settings, including permissions.

Training awareness in onboard personnel is a top priority and includes continuously training sessions during IT vessel operator's attendance. A provided form of IT Dept., like the relevant training forms, is completed by all attending personnel and records of training sessions are compiled in IT Dept. Furthermore, training sessions occur at office

in order to broaden cyber security awareness among others before Captains and Senior Officers taking up the reins of next vessel. Designated vessel operators are responsible for holding these sessions records of which are kept in IT Dept.
IT operators are appointed and clearly identified to all crew members onboard for any issues related to cyber safety.

ii. Third-party access.

Visits to ship by third parties requiring a connection to one or more computers onboard can also result in connecting the ship to shore. It is common for technicians, port officials, agents, pilots and others to board the ship and plug in devices, such as laptops and tablets and even use removable media to download data and perform other tasks. Below measure has been established.

Visitors PC. Each vessel is provided with a visitors PC that:

- Is not connected to vessel's LAN.
- Works in kiosk mode, i.e. system functions are inaccessible and with every restart the initial (and clean) state of the PC is restored.
- Any USB device can be plugged in and work.
- Restarting before every use is strongly recommended and labeled in visible location to encourage users to comply with.

iii. Regular backups of data.
To ensure data security onboard, it is highly recommended to make regular backups. External media such as external drives, recordable CD or DVD, are available to the crew for data backup. Such media must be stored in a location remote for the backed up system.

iv. Upgrades and software maintenance.
Use of hardware and software, which are no longer supported, should be carefully evaluated by IT Dept. as part of cyber risk assessment. Policy for timely updating of software is defined and enforced. The policy specifies what has to be updated, who is in

charge of these updates, as well as the means to obtain them. Updating procedures are monitoring by IT personnel.

v. Partition the network.
Without filtering equipment, each device has the ability to access any other and possible damages can easily spread to the entire network. Vital workstations, server, navigation and control systems of the ship are isolated physically or logically from other systems.

vi. Equipment disposal.
Obsolete equipment can contain data which might be commercially sensitive or confidential. Such obsolete equipment is returned to headquarters in order for IT personnel to properly destroy the data included prior to its disposal. In that way, vital information can be ensured and not retrieved.

7.3.3.3 VULNERABILITIES AND MITIGATION MEASURES
Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems which may be exploited, either directly e.g. weak passwords or indirectly e.g. absence of network segregation. When such vulnerabilities are exposed, there can be implications for confidentiality; integrity and availability of information as well as implications for safety of ship's critical systems. The following are cyber vulnerabilities, specifically for onboard IT Systems (both S/W and H/W) with detailed precautious measures to ensure their safety and integrity.

a) MS operating systems and MS Office:
i. MS Windows Server: operating system is updated, upgraded and maintained during IT Dept. attendance.

- Authentication required to login. Master is the only authorized user.
- No crew member has the right to access physically the server. In case the master is not in his cabin, the room is locked.
- Server is regularly restarted and cold started.
- Operating system's updates are disabled and user cannot install any updates.

- Provided with firewall and antivirus installations.
- Authorized external devises are used only.
- Locked in master's cabin.

ii. MS Windows OS: operating system and all executables are preinstalled from IT Dept. using a preconfigured image of latest windows ultimate edition.

- Windows firewall and defender is disabled in favor of Sophos antivirus.
- Operating system's updates are disabled and user cannot install any updates.
- USB's that are attached to devices with Windows OS are from IT Dept. and are used strictly for this purpose only. Personal USBs are strongly prohibited.
- For those that are connected to network, IT personnel have applied a fixed IP address.
- Software for the reinstallation in a pc can be found in IT CD Case left from IT vessel operator during his first attendance.

- MS Office: operating system is preinstalled from IT Dept using Microsoft Office latest or latest-by-one edition.
- Operating system's updates are disabled and user cannot install any updates.
- Macro command and running scripts are not allowed (disabled).
- Crew personnel are advised not to open email with attachments from unknown sources.
- Vessel files are to be stored either to servers shared folder named "Public" or in the same PC that have been created and used.
- Updates installed by Master using a simple script (batch command) which are provided occasionally via CD only from IT Dept.

b) Third-party applications:

i. Skyfile: is updated and upgraded by master and by IT vessel operator attendance.

- Vessel's email communication (incoming\outgoing) takes place from the vessel's
- Server only.
- Authorized email communication user is Vessel's Captain only.

- Internal email communication is authorized to limited users.
- IT-Dept. can provide internal or external email access.
- No crew member has the right to access physically the server.
- Master is the only authorized user to use Server.

ii. Software for Resting Hours and Performance: software is updated and upgraded by vessel's master and by IT Dept. personnel attendance.

- Data entered by authorized personnel only.
- All data entered are reviewed by vessel's master prior to submission to office.
- Master is the only authorized user to submit data reports.
- Data reports are transmitted to Office via vessel's Email software.

iii. Device Management System (DMS): software is updated, upgraded and maintained during IT Dept. personnel attendance and\or vessel's master.

- Access to NS5 is limited to authorized personnel.
- Data entered by authorized personnel only.
- Program software and program database are located in different drives.
- Program database is backed up in two different places (local drive and external drive).
- All data entered are reviewed/authorized by Vessel's Captain and/or Chief
- Engineer prior to submission to office.
- Replication files are transmitted to Office via Vessel's Email Software.
- Authorization is set by head Office (East med NS5 Support).

iv. Server and PC: software is updated, upgraded and maintained during IT Dept. personnel attendance and\or vessel's master.

- Software is updated and upgraded on regular basis automatically as set by Software
- Provider.
- Access to software settings is limited to authorized personnel.
- Authorized personnel is vessel's master.

- Software scans automatically and regularly for virus infections.
- Software automatically prompts for scan upon external device connection.
- Software prompts for update/upgrade action upon receipt.
- Server and network pc are automatically updated/upgraded.

1. Stand-alone Pc are updated\upgraded manually.
2. “How To” instructions are available onboard.

v. Adobe Acrobat Pro: software is updated, upgraded and maintained during IT Dept. personnel attendance.

vi. Operating System/ Service Console: software is updated, upgraded and maintained during IT Dept. personnel attendance.

- Access to software settings is limited to authorized personnel.
- Authorized personnel is vessel’s master.

vii. Tool for Program manager: software is updated, upgraded and maintained during IT Dept. personnel attendance and\or vessel’s master.

- Access to software settings is limited to authorized personnel.
- Authorized personnel is vessel’s master

viii. SMS Crew Mail Server and Client: software is updated, upgraded and maintained during IT Dept. personnel attendance and\or vessel’s master.

- Access to software settings is limited to authorized personnel.
- Authorized personnel is vessel’s master.

ix. SPOS: software is updated, upgraded and maintained during IT Dept. personnel attendance and\or vessel’s master.

- Access to software settings is limited to authorized personnel.
- Authorized personnel is vessel’s master.

x. Software for Performance: software is updated, upgraded and maintained during IT Dept. personnel attendance and\or vessel's master.

- Access to software settings is limited to authorized personnel.
- Authorized personnel is vessel's master.

c) Antivirus software:

i. Server and PC: software is updated, upgraded and maintained during IT Dept. personnel attendance and\or vessel's master.

- Software is updated and upgraded on regular basis automatically as set by Software
- Provider.
- Access to software settings is limited to authorized personnel.
- Authorized personnel is vessel's master.
- Software scans automatically and regularly for virus infections.
- Software automatically prompts for scan upon external device connection.
- Software prompts for update/upgrade action upon receipt.
- Server and network pc are automatically updated/upgraded.

1. Stand-alone Pc are updated\upgraded manually.
2. "How To" instructions are available onboard.

ii. Third party and contractors risk assessments

Self-assessments may be complemented by third-party risk assessment to drill deeper, and identify the risks and the gaps of their products that may not be found during self-assessment.

3rd Parties and collaborating contractors have been contacted by IT Dept., regarding the security that their products provide and have obtained evidence that they have taken satisfactory measures against cyber-attack. Documents of their responses are included in the system.

iii. Personal devices

Although USB flash drives are extremely useful devices for transferring data, they do come with security risks. They can contain malware and spread infections as soon as they are connected to a network. External devices can be used by intruders to bypass layers of defenses and can be used to attack systems that are otherwise connected to the internet. IT Dept. supplies each vessel with a sufficient number of authorized/approved USB flash sticks and an external HDD that can be used within the network PCs and the Server.

Use of other unauthorized USB devices will be rejected:

- A log is kept of such failed attempt.
- Only IT personnel have the authority and the technical tools to provide such legitimate USB devices.

7.3.3.4. SECURITY INCIDENT RESPONSE PLAN

A Security Incident means any incident that occurs by accident or deliberately that impacts your communications or information processing systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity or availability of information, data or services in this ***Company***. This includes unauthorized access to, use, disclosure, modification, or destruction of data or services used or provided by this ***Company.***

Indications of security breach are detailed in subsection 3.4.3.2.b.i:

a) A security incident response plan must be followed by all personnel. This includes all employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of the ***Company***, working with the ***Company*** or the customers' data or on ***the Company*** premises. For simplicity, all of these personnel are referred to as 'staff' within this plan. Staff may hold more than one role.

b) Roles.

The ***Company's*** Security Incident Response Team (SIRT) is comprised of:

Role	SIRT Responsibility	Name	Email	Telephone / Emergency telephone
IT Vessel Operator 1	Incident Response Lead			
IT Vessel Operator 2	Alternate Incident Response Member			
IT Manager	Incident Response Technical Lead			
Operations Department Manager	Operation Coordinator			
Responsible for Communications	Handling of any external communications in relation to an incident			

c) Responsibilities

i. The Incident Response Lead is responsible for:

- Making sure that Security Incident Response Plan and associated response and escalation procedures are defined and documented. This is to make sure that the handling of security incidents is timely and effective.

- Making sure that the Security Incident Response Plan is up-to-date, reviewed and tested, at least once each year.
- Making sure that staff with Security Incident Response Plan responsibilities are properly trained, at least once each year.
- Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Response Plan, as and when needed.
- Reporting to and liaising with external parties as is required.
- Authorizing on-site investigations by appropriate law security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.

ii. Security Incident Response Team (SIRT) members are responsible for:

- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the Incident Response Lead of an incident when they receive a security incident report from staff.
- Investigating each reported incident.
- Taking action to limit the exposure of sensitive or payment card data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing and analyzing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Resolving each incident to the satisfaction of all parties involved, including external parties.
- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.
- Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

iii. All staff members are responsible for:

- Making sure they understand how to identify and report a suspected or actual security incident.
- Reporting a suspected or actual security incident to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT).
- Reporting any security related issues or concerns to line management, or to a member of the SIRT.
- Complying with the security policies and procedures of ***this Company***. This includes any updated or temporary measures introduced in response to a security incident (e.g. for business continuity, incident recovery or to prevent recurrence of an incident).

d) Incident Response Plan Steps

There are a number of steps and stages that must be taken to make sure that the company is protected by reacting to a security incident appropriately.

i. Report

Information security incidents must be reported, without delay, to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT). The member of the SIRT receiving the report will advise the Incident Response Lead of the incident. In the event that a security incident or data breach is suspected to have occurred, it is recommended for staff to discuss their concerns with their line manager, who in turn may raise the issue with a member of the SIRT.

ii. Investigate

After being notified of a security incident, the SIRT will perform an initial investigation and determine the appropriate response, which may be to initiate the Security Incident Response Plan. If the Security Incident Response Plan is initiated, the SIRT will investigate the incident and initiate actions to limit the exposure of cardholder data and in

mitigating the risks associated with the incident. Initial incident containment and response actions.

iii. Inform

Once the SIRT has carried out their initial investigation of the security incident:

 The Incident Response Lead will alert the SIRT's senior management primary contact.

 The Incident Response Lead and/or the SIRT personnel responsible for communications/PR will inform all relevant parties. This includes the acquirer and local law enforcement, and other parties that may be affected by the compromise such as customers, business partners or suppliers. This also includes the personal data breach notification contacts, as applicable to the incident under investigation.

iv. Maintain Business Continuity

The SIRT will engage with operational teams to make sure that company can continue to operate while the security incident is being investigated.

v. Planning

In advance of any security incident that may impact the company, a plan must be made for how business would operate if the systems and processes were unable to operate as normal.

Such planning should include:

- System and data backups available in the event of loss of data, system corruption/virus infection or hardware failure.
- Offline or alternative payment acceptance methods should be used if company is unable to take card payments on ecommerce website, in-store or over the telephone using the usual methods.

vi. Resolve

The SIRT will liaise with external parties, including the acquirer, law enforcement,

etc., to ensure appropriate incident investigation (which may include on-site forensic investigation) and gathering of evidence, as is required.

The members of the SIRT will take action to investigate and resolve the problem to the satisfaction of all parties and stakeholders involved. This will include confirmation that the required controls and security measures are operational. The Incident Response Lead will report the investigation findings and resolution of the security incident to the appropriate parties and stakeholders (including the acquirer, local law enforcement, etc.) as is needed.

vii. Recovery

The Incident Response Lead will authorize a return to normal operations once satisfactory resolution is confirmed. The SIRT will notify the rest of the company that normal company operations can resume. Normal operations must adopt any updated processes, technologies or security measures identified and implemented during incident resolution.

viii. Review

The SIRT will complete a post-incident report, IT Cyber Security Incident Reporting Form, after every security incident. The purpose of this form is to document how the incident occurred, what the root causes were and how well the incident was handled. This will help to identify recommendations for better future responses and to avoid a similar incident in the future.

Changes and updates that may be required include:

- Updates to the Security Incident Response Plan and associated procedures.
- Updates to Company's security or operational policies and procedures.
- Updates to technologies, security measures or controls (for example, improved measures to inspect payment terminals for card skimmers).
- The introduction of additional safeguards in the environment where the incident occurred (for example, more effective malware protection).

The SIRT Executive Officer/Risk Owner (the senior management primary contact) will ensure that the required updates and changes are adopted or implemented as necessary.

7.3.4 REFERENCES (…)

7.3.5 DEFINITIONS (…)

7.3.6 RECORDS

I. Computer application records.
II. Inventory of all H/W and computer peripherals.
III. Current Data Back-ups.
IV. Directory of approved Suppliers.
V. H/W & S/W Licenses and Contracts.
VI. Outstanding work-lists by the IT department per vessel.

7.4 VETTING INSPECTION

Vetting inspection is a grading system of a ship, enabling a potential charterer to compare between similar ships and choose the best for his needs, to maximize efficiency (Souvlas, 2014). Many years before the oil industry has started to concern the safety of carrying their products via oil tanker vessels, so they created a big platform system for every available and secure vessel in the oil industry, based on a well-known convention such as MARPOL, SOLAS and STCW convention.

Nowadays, a charterer when he/she wants to choose a ship and finds something interesting for carriage the goods, he/she will search the history of the company, the history of the vessel and generally the entire fleet, previous fixtures, etc. to make sure that it will be all in order after their fixture/contract. As we know, this market is very competitive and all the ship owners have to compete each other for their position in the market and “hit” the highest prices (freight rates, etc.) especially in pick seasons. So, the first that they have to do is to ensure and warranty that all of their vessels’ certificates, crews certificates, cargo papers, vessels’ records and all the machineries, systems and alarms onboard are in the best condition. Meanwhile, whenever an inspection is scheduled or announced, the Master of the vessel and the Marine Superintendent or the

Port Captain have to prepare and show to the Inspectors all the documents, papers, certificates and a specific questionnaire, the VIQ (Vessel's Inspection Questionnaire).

One of the last added section on the vetting questionnaires was the Cyber Security onboard. As this issue concerns the oil industry as much as the general maritime industry. Every oil company wants to ensure that every vessel is cyber-seaworthy and there is nothing in danger to concern about.

7.4.1 QUESTIONNAIRES

Oil Companies International Marine Forum (OCIMF) was formed in April 1970 in response to the growing public concern about marine pollution, particularly by oil, after the Torrey Canyon incident in 1967 (OCIMF, 2019). Moreover, OCIMF presents the oil industry in every IMO meeting all these years and cooperates with governments and intergovernmental bodies (i.e. IMO, EUNAVFOR, UKMTO, ReCAAP, NATO, etc.). OCIMF is the voice for all the major oil companies including the majority of national oil companies for issues like environmental concern, maritime security in sea, etc. Also, OCIMF has introduced a new guidance on pressing current issues such as piracy and Arctic shipping, except the guidance the big role that OCIMF has played in a substantial quantity of regulation at the IMO regarding the safety of tankers and the environmental protection of seas.

In addition OCIMF has published quite a few but the most important documents/guidance for maritime security to protect mostly the seafarers, including its Ship Inspection Report (SIRE) programme and Tanker Management and Self-Assessment tool (TMSA). Although, with OCIMF's help and approach all these years, the maritime sector was helped to recognize every kind of piracy and so much guidance tools in case of a threat. The hot topic on their agenda is the Maritime Cyber Security, nowadays, and as they work of the publication of the IMO's Guidelines on Cyber Security Onboard ships, they keep going for new amendments or approach on this issue.

OCIMF's Maritime Security Publications:

- BMP5 Best Management Practices to Deter Piracy and Enhance Maritime security in Red Sea, Gulf of Aden, Indian Ocean and Arabian Ocean, 2018.
- Global Counter Piracy Guidance for Companies, Masters and Seafarers, 2018.
- The Guidelines on Cyber Security Onboard Ships, 2017.
- Guidelines to Harden Vessels, 2018.
- Guidance for Oil Terminal Operators on the IMO International Ship and Port Facility Security (ISPS) Code, 2003.
- Piracy and Armed Robbery Against Ships, 1st Edition, 2000.
- Regional Guide to Counter Piracy and Armed Robbery against Ships in Asia, 2016.
- Ship Security – Bridge Vulnerability Study, 2014.

OCIMF - Vessel Inspection Questionnaires for Oil Tankers, Combination Carriers, Shuttle Tankers, Chemical Tankers and Gas Tankers, Seventh Edition- VIQ 7 (22 February 2019).

Here is a part of a typical questionnaire during a vetting inspection:

7.14 Are Cyber Security Policy and Procedures part of the Safety Management System and is there a Cyber Response Plan onboard? Note: Do the procedures include a risk assessment of issues such as:

• Threats such as from malware; phishing attacks etc.

• Identification and protection of vulnerable systems (ECDIS etc.)

• Mitigation measures, (USB control etc.)

• Identify key personnel within the company (including who the master reports suspected incidents to)

• Hard copy of key contacts (e.g. DPA; CSO etc.).

• Password management/record? • Contractor compliance Note: Does the Cyber Response plan contain guidance on:

• What ‘symptoms’ to look for,

• Immediate actions to be taken and

• Name, position, phone number and email for the Responsible Person to be contacted

7.15 Are the crew aware of the company policy on the control of physical access to all shipboard IT/OT systems? Note: Inspectors should observe if access to USB ports on 'Shipboard IT/OT' terminals are controlled (i.e. there are measures in place to block/lock USB/RJ-45 ports on these terminals. Procedures should include the protection of Critical equipment such as ECDIS from malware and virus attacks. Procedures should include the control of access to all shipboard IT/OT terminals including access to Servers which should be in a secure location. The procedures should also include access by any third-party contractors and technicians.

7.16 Does the company have a policy or guidance on the use of personal devices onboard? Personal devices include phone/tablets etc. and storage devices such as USB sticks. Check if the policy is implemented by both, crew and visitors, e.g. all third-party contractors and technicians.

7.17 Is Cyber Security awareness actively promoted by the company and onboard? Note: Active promotion might include:

• 'Cyber Awareness Material' displayed by all IT terminals and in crew rest rooms • Training films shown to crew

• Crew specific training VIQ 7 – 17 September 2018 75

• Instruction on safeguarding of passwords

• Responsible use of social media.

• Policy on the use of personal devices and its inclusion in shipboard joining familiarization checklists.

• May include companies own employee/contractor Authorized User Policy (AUP) agreements.

• Company certified as per ISO 27001.

Also, there is an Inspection and Assessment Report For Dry Cargo Ships (FOD06) (Rev.11 Date 11 May 2017) for Cybersecurity:

4.7.1 Does the vessel and/or company have documented software/firmware and hardware maintenance procedures?

4.7.1.1 Are service reports available?

4.7.2 Does the vessel and/or company have any cyber security procedures?

4.7.2.1 Has a Risk Assessment for Cyber-attack been completed?

4.7.2.2 Is a Cyber-attack Response Plan available?

4.7.3 Does the vessel and/or company provide any cyber security training?

8. AUTONOMOUS SHIPPING

8.1 INTRODUCTION

The terms “autonomous” and “unmanned” are used in different texts, sometimes to mean the same thing and sometimes used individually with different meanings in different texts. The Norwegian Forum for Autonomous Ships proposes the following principle for using terms:

• ***Autonomous*** means that the ship can perform a set of defined operations with no or reduced attention from a bridge crew. This does not necessarily mean that no human is present.
• ***Unmanned*** means that there is no human present on the ship’s bridge to perform or supervise operations. Crew may still be on board the ship.

In the early 1970s, ship technology improved with the unmanned engine room, satellite navigation, anti-fouling paint finishes, more efficient diesel engines, vastly improved hatch covers and a host of other technical improvements in the design and construction of

merchant ships. Automation and reliable monitoring systems have played an important part in reducing crew numbers. It is now common practice for the engine room to be unmanned at night, and various other systems have been introduced such as remote control ballast, single man bunkering, rationalized catering and improved communications which remove the need for a radio officer (Stopford, 2009).

Technological advances in the shipping industry, such as autonomous ships, drones and various block chain applications, hold considerable promise for the supply side of shipping. However, there is still uncertainty within the maritime industry regarding possible safety, security and cybersecurity incidents, as well as concern about negative effects on the jobs of seafarers, most of which come from developing countries.
While the development and use of autonomous ships offer numerous benefits, it is still unclear whether this new technology will be fully accepted by Governments, and particularly by the traditionally conservative maritime industry. There are legitimate concerns about the safety and security of operation of autonomous ships and their reliability. The diminishing role of seafarers and ensuing job loss are a particular concern (UNCTAD, 2018).

The maritime transport industry is increasingly playing catch-up when it comes to enhancing the use of innovative technologies to improve systems and processes. One industry survey reveals that according to 15 per cent of respondents, autonomous terminal equipment was already being used (Vonck, 2017).

The IMO has adopted a decision with regard to regulatory scoping exercises to establish the extent to which the international regulatory framework should be modified to integrate the new technology involving maritime autonomous surface ships.
The term “autonomous ship” is not the same as “unmanned ship”, as the former may operate at various levels of autonomy, including partially autonomous (with human input) and fully autonomous (not requiring human intervention). However, such terms have not yet been completely defined either nationally or internationally, and many different formulations exist of the levels of autonomy (Danish Maritime Authority, 2017)

The first remotely controlled or fully autonomous commercial cargo vessel may be in operation by 2020; for example, the first fully electric and autonomous container ship, with zero emissions, may be in operation on a short coastal route in either a remotely controlled or autonomous mode by 2020 (Marine Electronics and Communications, 2018b)

The benefits mainly derive from the removal of the human element which may reduce associated errors; and provide financial savings on crew salaries and omission of crew accommodation. However, even though the technical concepts for unmanned vessel operation are well established, studies on human interaction with the systems are not as prevalent (Hogg, Ghosh, 2016).

The technology may first be deployed on vessels that undertake coastal and short sea routes, and remotely controlled and autonomous ships sailing open oceans could be in operation by 2030 or earlier. An autonomous, fully battery-powered short sea vessel with zero emissions is also currently in development (DNV GL, 2018).

Other recent developments with regard to autonomous ships include the following: a prototype of the world's first fully autonomous and cost-efficient vessel for offshore operations (Kongsberg, 2017); the first electrically powered inland container vessel in Europe, with five small ships in the series expected to be completed in 2018 and six larger ships in preparation with features that prepare them for autonomous operations (*The Maritime Executive*, 2018); an agreement between two companies, possibly a first in the marine sector, to develop an artificial intelligence-based classification system for detecting, identifying and tracking the objects a vessel can encounter at sea, aimed at making existing vessels safer and progressing towards making autonomous ships a reality (Rolls-Royce, 2017); the One Sea autonomous maritime ecosystem project, aimed at enabling fully remote-controlled vessels in the Baltic Sea by 2020 and achieving autonomous commercial operations by 2025 (IMO, 2018b); and the testing of remotely controlled vessels in the Pacific Ocean, due to begin in 2019, aimed at achieving autonomous vessels by 2025 (Bloomberg, 2017).

A ship operating autonomously without any human oversight would not be able to comply with such provisions and, should an incident occur, issues related to safety and liability might arise. Such functions may have to be taken over by shore-based staff

supervising remote-controlled or autonomous ships, and many of the liabilities may have to be assumed by ship-owners, shipbuilders and manufacturers of ship components, as has been addressed in similar situations involving autonomous vehicles (The Conversation, 2018b).

There are few enough levels of automation in the shipping sector's mind until now. Although, for some companies, there are up to five or six levels of automation but the most common and acceptable for everyone in the industry are approximately up to four levels of autonomy.
A ship's autonomy levels are categorized on a specific scale:
Level 0 - Conventional ship:

- Fully manned ship
- Humans acquire and analyze data, make and execute decisions

Level 1 – Smart ship:

- Directed by humans
- Relies on systems and sensors for support in collecting data and making decisions

Level 2 and 3 - Semi-Autonomous ship:

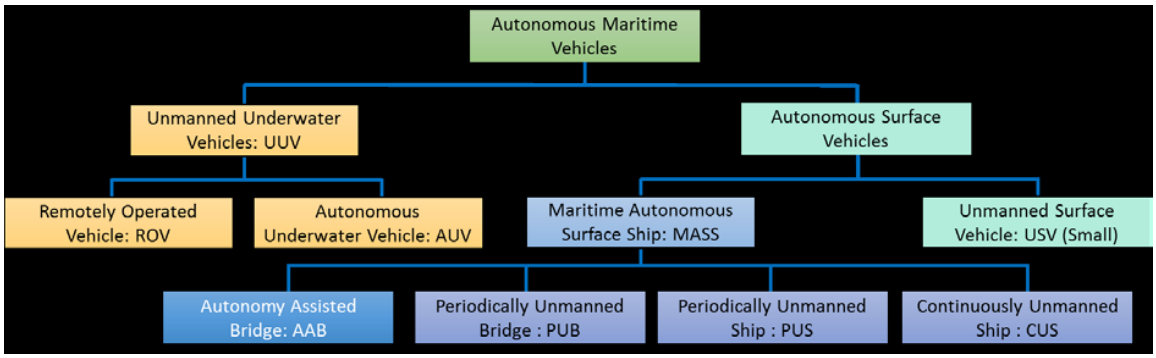
- Human delegated or supervised
- Relies on systems to make decisions and/or initiate actions

Level 4 – Fully autonomous ship:

- Unmanned ship
- Requires no input from humans other than in an emergency

There are a lot of approaches regarding the levels and the types of autonomous vehicles, vessels, etc. The maritime industry have tried to define all these levels, sometimes in more specific details and others with a few, depending on the needs for everyone in this sector.
Another one approach for NFSA's side is the Maritime Autonomous Surface Ship (MASS), which has already been suggested as a general term for autonomous ships. This needs to be subdivided into different classes that have different impact on operation and legislation:

- ***Autonomy Assisted Bridge (AAB) / Continuously manned bridge*:** The ship bridge is always manned and the crew can immediately intervene in ongoing functions. This will not generally need any special regulatory measures except perhaps performance standards for new functions on the bridge.
- ***Periodically Unmanned Bridge (PUB)*:** The ship can operate without crew on the bridge for limited periods, e.g. in open sea and good weather. Crew is on board ship and can be called to the bridge in case of problems.
- ***Periodically Unmanned Ship (PUS)***: The ship operates without bridge crew on board for extended periods, e.g. during deep-sea passage. A boarding team enters or an escort boat arrives to control the ship, e.g. through the port approach phase. For regulatory purposes, this would probably be the same as CUS.
- ***Continuously Unmanned Ship (CUS)*:** The ship is designed for unmanned operation of the bridge at all times, except perhaps during special emergencies. This implies that there are no one on the ship that are authorized to take control of the bridge, otherwise, the ship would be classified as PUB. There may still be persons on the ship, e.g. passenger or maintenance crew.



Source: NFSA - Classification of autonomous maritime systems and autonomous ship types

8.2 THE MUNIN PROJECT

The MUNIN research project has developed a technical concept for the operation of an unmanned merchant ship and assessed its technical, economic and legal feasibility. The concept‘s core is a ship which is completely unmanned at least for parts of the voyage.

Furthermore, the project aims for short-term exploitation potentials to support the technological progress in conventional shipping (European Commission, 2016).
MUNIN was proposed as a concept, where the ship is autonomously operated by new systems on board the vessel, but the monitoring and controlling functionalities are executed by an operator ashore.
In the MUNIN project they experimented on a dry bulk carrier of 75.000 dwt, operating in a long continuous deep-sea voyage, at a service speed of 16 knots. The part of the voyage in congested or shallow waters was not a part of the MUNIN project, because they believed that this part still will need to be executed by a crew on board of the vessel (Pol Deketelaere, 2017).
Thus, the MUNIN concept defines the following systems and entities and implemented them as prototypes:

• An Advanced Sensor Module, which takes care of the lookout duties on board the vessels by continuously fusing sensor data from existing navigational systems combined with modern daylight and infrared cameras;
• An Autonomous Navigation System, which follows a predefined voyage plan, but with a certain degree of freedom to adjust the route autonomously, e.g. due to an arising collision situation or significant weather changes;
• An Autonomous Engine and Monitoring Control system, which enriches ship engine automation systems with certain failure-pre-detection functionalities while keeping the optimal efficiency;
• A Shore Control Centre, which continuously monitors and controls the autonomously operated vessel after its being released from its crew by its skilled nautical officers and engineers (MUNIN, 2016).

Also, the high-level objectives of the MUNIN design process are:

- Ensure an acceptable safety and security level for own and other ships and the international shipping community in general.
- Minimize uncertainty in the missions' intended outcome as well as in unintended side effects.
- Develop a cost effective system that can compete at a level field in a commercial operational environment (TransNav, 2015).

8.3 REGULATION AND THE LEGAL FRAMEWORK

Any autonomous vessel should be compliant with all relevant regulations from international conventions adopted by IMO or from local legislation. If necessary, exemptions or equivalent solutions should be explicitly approved by the Administration (BV, 2017).

In relation to the regulation of cyber security in shipping, it should be considered to establish special obligations for ship owners to report cyber security incidents to the flag State. Subsequently, the flag State could share knowledge about the type and number of cybersecurity incidents in anonymized form with other flag States as well as the ship-owners and other relevant stakeholders, such as classification societies and insurance companies with a view of acquiring a better knowledge based on countering and planning a preparedness against cybersecurity incidents.

For example, in Danish law, section 4(3) of the act on safety at sea contains the legal basis for the Minister for Industry, Business and Financial Affairs to *"lay down regulations on the obligation to report accidents and other incidents at sea to the Danish Maritime Authority as well as information about the authorities' reporting hereof to the European platform for accidents at sea"*. This legal basis could be used for issuing regulations on reporting obligations in connection with cyber security incidents.

These are already risk factors that are becoming increasingly relevant for traditional ships, but the current safety regime is not adequately handling these risks, mainly relying on human fallback and a partly false dependence on redundancy. For autonomous and remote-controlled ships, this deficiency in the safety regime will become even more evident, and likely unacceptable from a risk perspective. In addition, the vulnerabilities of software-based systems to cyber threats also represent an increased risk. The question is then: How should the safety regime be designed to ensure safety assurance for such systems? However, cyber security risks are not static, and requirements, verification procedures and counter measures must be continuously updated to reflect the developing threat, particularly related to remote-controlled and autonomous ships. (DNV GL, 2018)

8.3.1 IMO

The biggest regulatory organ within the maritime industry is the International Maritime Organization (IMO). IMO has not yet been convinced that autonomous shipping is safe, so there are still no common regulations for autonomous ships. Development of regulations is expected to start in the late 2017 (Petteri Vistiaho, 2017).

The IMO should have to review any existing regulation and amend it by the provisions of autonomous vessels. So, the IMO's senior technical body, the Maritime Safety Committee (MSC), after their meeting in May 2018, endorsed a framework for a regulatory scoping exercise, as work in progress, including preliminary definitions of Maritime Autonomous Surface Ships (MASS) and degrees of autonomy, as well as a methodology for conducting the exercise and a plan of work (IMO, 2018).

8.3.2 DNV GL

DNV GL has published the guidelines for "Autonomous and remotely operated ships" in September 2018 which contain methods, technical requirements, principles and acceptance criteria related to classed objects as referred to from the rules, fully including any principle that arises from the issue of autonomous vessel. For example, the vessel's design and every system in which it consists, from the engine to the bridge, the vessel's safety and quality through the navigational systems, the vessel's communication systems, the cyber security of the vessel, etc.

The increased communication between the vessel and remote systems is bringing with it a concern about the cyber security for the related systems. In order to address this concern, the guideline puts emphasis on securing the systems when it comes to cyber security. Both the concept qualification process and the technology qualification process includes cyber security aspects in the risk analysis, and the technical guidance for the communication link references both the type approval programme for cyber security and the cyber security class notation. The general rule is that a defence in depth concept should be applied, where multiple layers of mechanisms, functions and barriers together aim at hindering, detecting and limiting the damage of cyber security breaches. Incidents related to cyber systems should be considered in the risk assessments. (DNV GL, 2018).

As it is clearly stated in this guidance, the cyber security and the issue of cyber-attacks are one of the main concerns for the autonomous vessels. Because, the main aspect is the automation systems that will be on those vessels and as we all think, the fully automated vessels will be more “unprotected” than others, since there will be no human element on every autonomous vessel or the few seafarers that will be there, may not be enough for protecting the vessel on a potential cyber-attack.

8.3.3 SOLAS

A new code would be a simpler and more practical option, even though many of the same challenges for a new convention would be relevant for a new code. However, if the code was made mandatory under SOLAS (with a new SOLAS chapter as an anchoring point), the use of the code would have the same application as a convention. If the code was mandated by a two-thirds majority, ratification challenges would be avoided. Even if it is decided to develop a new convention or code, amendments of other regulatory instruments must take place where these contain explicit showstoppers (DNV GL, 2018).

8.3.4 CONCLUSION THOUGHTS

The phrase ‘No seafarers no sea trade’ view expressed by the eminent maritime lawyer Mr. Puttfarken in 1997 appears at the very least to be fundamentally mistaken. The impact on the shipping industry of the replacement within the proximate future of the hard work of masters, ships’ officers and crews by computer programs and artificial intelligence, assisted at most by shore-based vessel controllers has the potential to change the social and economic parameters of the shipping industry as much as the introduction of steel construction and steam propulsion did in the nineteenth century.

On the other hand maritime law with its long history appears on first examination to be relatively well armed for this technological innovation, and the necessary and undoubtedly extensive adaptations of existing public and private maritime law will be unlikely to bring about a revolution.

Maritime law will not die out but will enter a new phase of development, once again proof of the continuity and necessity of this branch of the law (Van Hooydonk, 2014).

8.4 DETECTION, RESPONSE AND RECOVERY AFTER A CYBER-ATTACK

"The present state of SOLAS and collision avoidance regulations are being over taken by and holding back potentially industry-changing technology from being developed and implemented,", Joe Walsh, Partner at Clyde & Co.

Monitoring should be in place to detect abnormal events or intrusion such as massive data transfers (depending on usual operating modes), several log-in failures to an active or inactive account.

In the event of an incident, a contingency plan should be defined for working in downgraded mode. The first measure should be to isolate all infected machines from the network. For each incident, a feedback should be capitalized in order to be more effective in dealing with a similar event in the future. Essential information and software backup facilities should be available for recovering to a clean system (BV, 2017).

8.5 INSURANCE COVERAGE

"...It is probably worth mentioning that the maritime industry as a whole has been criticized for being a bit slow in reacting to existing cyber threats, including fully crewed vessels and that the biggest threat to any organization's cyber-security posture is still, in fact, human error. It is therefore possible that a transition to unmanned ships might actually reduce an organization's profile and exposure to cyber risks, ", Mr. Walsh.

Cyber insurance products have been developed, but it is uncertain whether the coverage needed is available in relation to the actual risk and extent of loss since present cyber insurance products have the form of collective arrangements (pools), where one ship-owners major loss could exhaust the other insurance-covered ship-owners possibility of being covered.

Cyber insurances do not yet have an extent where there is a secure insurance market. Furthermore and according to the insurance companies, there is a large gap between the actual cyber risk and the limited insurance taken out in this field and, thus, a major non-insured risk (Danish Maritime Authority, 2017).

Moreover, Clyde & Co points out that the International Union of Marine Insurance (IUMI) has been discussing the implications of the new technology. While there are not

yet any concrete answers, IUMI expects unmanned vessels to change the landscape of the traditional maritime insurance industry (The Maritime Executive, 2017).

9. GDPR

Reflecting the need of a more enhanced cyber protection, after all of those incidents in a lot of sectors, for example in logistics, in the maritime industry, in commercial fields, etc., the EU set in force the GDPR regulation in May 2018, which updates and upgrades current data protection legislation by requiring businesses who deal with EU citizens -and shipping organizations included- to be transparent about how they use their data (Safey4Sea, 2018). The GDRP is the first comprehensive overhaul and replacement of European data protection legislation in over twenty years and could be the most significant regulatory framework to hit organizations since Sarbanes-Oxley in 2002 (Secureworks, 2018).

9.1 INFORMATION COMMISSIONER'S OFFICE (ICO)

The UK's supervisory authority for the GDPR is the ICO who is responsible for promoting and enforcing the legislation, as well as providing advice and guidance to organizations and individuals. The ICO has published a lot of helpful guidance on its website. This should be your first port of call for any overarching GDPR queries you might have (NCSC, 2018).

The GDPR requires that personal data must be processed securely using appropriate technical and organizational measures. The Regulation does not mandate a specific set of cyber security measures but rather expects you to take 'appropriate' action. In other words you need to manage risk (NCSC, 2018).

This new regime would imply a completely different approach regarding the security measures than the current regime in force, for instance, in Spain. Spanish legislation on data protection includes, within its developing regulations, the technical standards legally required so as to determine whether

the measures implemented and in force are appropriate to safeguard the use and access to the relevant data processed by the relevant company.

However, the Regulation sets the duty/burden on companies to assess and decide what type of measures they shall put in place instead of just following the applicable legal requirements. This new approach would lead to a scenario in which the security measures implemented by a company would only be checked by the authorities in case a data breach arises. Therefore, companies should implement measures that are at the forefront of the art and should be able to evidence that those measures were enough to avoid, as much as possible, any potential data breach.

The General Data Protection Regulation is also based on the privacy by design principle. This principle states that any product or service shall be designed from the very beginning with data minimization standards in mind. Therefore, businesses shall warrant and limit the processing of personal data only to the strictly necessary extent to achieve the purpose for which the data is gathered; and the access to such data shall be limited to those who need it for the execution of their duties. (*Financier Worldwide, 2016).*

Under the GDRP we have the obligation to report and notify the ICO, for every incident or personal data breach that we thought we are affected. Moreover, the ICO provides a detailed guidance about what constitutes a notifiable breach, preparing and responding to breaches.

Although, incidents below national threshold should be reported to Action Fraud, the UK’s national fraud and cyber-crime reporting center or, if you're in Scotland, then reports should be made to Police Scotland (NCSC, 2018).

10. RISKS AND CONSEQUENCES AFTER A CYBER-ATTACK

10.1 INTRODUCTION

The lack of a Cyber Security Strategy for the industry has to be addressed as a matter of urgency. Common policies, procedures and processes are required to be developed and installed to reduce the threat attack to individual vessels, offshore installations, common maritime systems and onshore facilities. In addition to individual attacks the industry is also susceptible to acts of terrorism through breaches of security as noted below (Garcia-Perez, Thurlbeck, How, 2018).

In general, most maritime vessels are run by outdated software using hardware that was not designed with cyber security in mind. This is the result of the timescale and cost of producing large ships, but results in largely vulnerable systems. Both security firms and hackers have found both general flaws and specific, real-world, flaws within the systems running in the maritime industry. Specifically, several successful cyber-attacks have been launched on the navigation systems of ships. However, as these systems were not designed to be securely isolated, it seems plausible that similarly outdated systems for propulsion and cargo handling may also be compromised and abused by cyber-attackers (Tam, Papadakis, Jones, 2012).

10.2 SAFETY

Some years before, Al Qaida and other terrorist groups have stated intent and capability to attack vessels, perhaps best illustrated in the attack on the USS Cole off Aden in 2000 by al-Qaida in the Arabian Peninsula (AQAP). More recently, AQ-linked strategist Suleiman al - Ali published a chapter on ‘Maritime Jihad’ in his online book, ‘The Fall of the Idol’. He describes targeting commercial shipping as being the best path for Mujahidin to gain control over the global economy.

Terrorist groups have increased their use of the internet for operational and radicalization purposes, using it for encrypting operational communications and sharing radicalizing content. Although their use of cyber-attacks for destructive or disruptive purposes remains nascent, targeting maritime-related assets has been noted. In July 2016, the Caliphate Cyber Army released databases belonging to shipping companies. Three

companies were targeted and data released on containers shipped into and out of the Suez Canal Container Terminal (Garcia-Perez, Thurlbeck, How, 2018).

The vulnerabilities created by accessing, interconnecting or networking every companies' systems can lead to cyber risks which should be addressed to every employee or seafarer to be aware and ready to face every problem and threat which can lead to a cyber-attack. Some of the vulnerable systems could include, but are not limited to:

- Communication systems
- Bridge systems
- Cargo handling and management systems
- Propulsion and machinery management and power control systems
- Access control systems
- Administrative and crew welfare systems.

Moreover, cyber risks may also occur from various sources. For example:

- ❖ Malicious actions, e.g. unauthorized access or malicious attacks to ships' systems and networks
- ❖ Legitimate actions, e.g. software maintenance or user permissions, updates
- ❖ Case were risks are neglected e.g. personnel having access to the systems onboard, for example by introducing malware via removable media.

The safety, environmental and commercial consequences of being unprepared from a cyber-attack may be significant.

Technologies and cyber threats are rapidly changing, making it difficult to address these risks only through technical standards. So a risk management approach, which translates to human awareness, is necessary.

The maritime industry has already seen the threat demonstrated in recent cyber-attacks resulting in huge revenue losses. However, the possible effect of a cyber-attack on the safety of the ship's operation becomes increasingly critical when the operational ship functions are controlled by software and control signals sent through a communications link (DNV GL, 2018).

10.3 ECONOMIC

The most common issue between every cyber-attack and in every hacker's mind is the economic cause for their targets. We can imagine the losses for the COSCO's cyber-attack, few years before, or the losses from the Saudi Aramco's incident. In most of the times, such as these cases cause hundreds or millions of dollars. Some companies could be able to survive after a cyber-attack, some others could be bankrupt. Moreover, together with the economic losses are the reputational issues, which can face a company after a cyber-attack. Directly, the cyber-attacked company is showing weak to every company in the maritime industry, cooperating or competing companies. As a result, after their restoration maybe the losses would be more and more, as time goes by, on their clients and the time for them to win them back could be bad and risky for these companies.

10.4 ENVIRONMENT

Environmental pollution is another one potential risk related to cyber security and cyber-attacks. As a consequence, after an incident of a cyber-attack, for example a collision after hacking a monitoring system of a fully-loaded tanker vessel can lead to a massive environmental pollution, a big oil spill in an ocean, like the well-known accident of oil spill, the M/T Exxon Valdez, twenty years before in 1989, which has spread approximately 37,000 metric tons of crude oil. In addition to, in a potential cyber-attack on a vessel could lead also to an air pollution phenomenon, etc.
So, the physical damages could be a variety of phenomena for the environment and the consequences could be different on every case.

10.5 CONCLUSION THOUGHTS

As with most operational environments without developed understanding of cyber-attack vectors, the most likely introduction of malware will be inadvertent. Infected media being brought aboard and used to update equipment is a threat seen elsewhere in the enterprise. Blended attacks are likely to continue to appeal to criminals and terrorists and develop in sophistication and audacity. The confluence of technology and physical attack is already

present in terrorist and criminal operations. Monitoring terrorist adoption of destructive cyber capability should be considered with maritime threats in mind, given the continued interest in targeting shipping (Garcia-Perez, Thurlbeck, How, 2018).

So, in our minds we have to understand that the phenomenon of cyber-attack could lead to different consequences and every cyber-attack has its own risk and result. In every hackers' mind there is a different reason of creating a virus or to steal personal information data or steal from their victims their bank accounts' details. The benefit, the target, the method and the result almost all the times differ between its other.

11. CONCLUSION

The risk of a cyber-attack was increased all these years, from the end of the 20th century up to now, when the internet has arrived and forced to be a part in our lives and jobs. The digitalization, as a result, has been in an increasing level every year with a lot of achievements too. But as every issue has both sides and results, the technology made our everyday lives easier but became more vulnerable to third parties. So, the same happened to the maritime sector. It is so easy to see and monitor a vessel now than three decades before, when a vessel started its journey to crossover the oceans and no one from the seafarers' families could be able to see or know where the vessel was or when the vessel would be able to arrive at the destination port. But nowadays, as a common person, outside the maritime world can see any vessel via the vessel's AIS system, the same could be able to do a hacker. So the targets become more and more vulnerable to this system. It is remarkable to say that cyber awareness become important in our working lives, as the maritime sector be awake in those threats and risks of a cyber-attack. There are still vulnerable points within some essential systems that provide an open door to walk through an attacker or in other words a hacker, causing several and devastating consequences to their victims or targets by discovering their vulnerable sides.

Historically, the sea has been one of the most important conduits of economic prosperity. Due to the inherent dangers of the maritime environment, maritime terrorism, trigger happy hijackers and sea pirates, negligent mariners and, now, cyber-criminals, the

shipping industry must be more vigilant than ever if the global economy is to be sustained (Professor Vivian Louis Forbes, 2018).

Any hacker before an attack has to investigate and find his or her victim's sensitive point. The most vulnerable attack point related to cyber-attacks and generally to cyber security is people. Surely, the cyber world is everywhere and is provoked from every criminal to enter in. There are a lot of reports regarding cyber-attacks. The human factor is inextricably linked with the cyber world, because employees handle the monitoring systems of a vessel, or the communication systems of a company, or the financial projects and details of any company, etc. and all of them are inside and linked to any computer system, in simple words.

Therefore, any cyber strategy needs management to be involved in the decisions relating directly to the level of security a company wants, as increased levels of cyber security comes at the price of having to modify business processes (MTI, 2019).

There is an awareness of the ways that digitalization projects expand the attack surface, but it also needs to include a reevaluation of our broader strategies and the tools we're relying upon. Luckily, technology capable of autonomously fighting back against cyber-attackers already exists. The onus is now on industrial centers, from ports to oil rigs, to fight to stay one step ahead of our evolving adversary (Justin Fier, 2018).

As we can see in recent years and developments, there is no zero cyber risk environment. There is a common problem to perceive their actual defense ability and the state of the circumstances that they were locating in, the general cyber awareness was therefore proved insufficient. It is suggested that individual shipping companies could formulate their cyber-security training programme based on their particular employee needs, in which the factor of different role and working years could be taken into consideration. For example, a tailor-made cyber-security training programme could be made for offshore employees, address their differences between offshore and onshore company such as the IT reporting system. By eliminating individual uncertainty, it can help to ensure the awareness level of employee (Kelvin Pang, 2017)

To sum up, the current challenge is that no practical guidelines are in place for the maritime sector, and given the global nature of the maritime industry, nationally mandated guidelines are highly likely to become conflicting and hence counterproductive as vessels move across different national jurisdictions (Lars Jensen, 2015). The cyber awareness is the most important key that could change and minimize the cyber-attacks' world. Every company in the global trade industry has to train and protect their properties and reputation by training any of their employee and organizing their systems from a professional view, the more the criminals the more the protected companies.

12. REFERENCES

Books:

Chartering Manual by Practitioners, by Th. Pagonis, N. Pentheroudakis, P.B.A. LLP, 2019

Database System Concepts, by Silberschatz, Korth and Sudarshan, 6th edition, 2010

Websites:

https://safety4sea.com/cm-the-cyber-risk-landscape/

https://safety4sea.com/maritime-cyber-attacks-still-reality/

https://commons.wmu.se/cgi/viewcontent.cgi?article=1662&context=all_dissertations

http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

https://www.mtinetwork.com/category/news/cyber-security/

https://safety4sea.com/watch-cyber-attacks-pose-great-threats-in-maritime-industry/

http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx

https://www.hellenicshippingnews.com/cybersecurity-and-maritime-industry/

https://securestatecyber.com/cyberbloggen-en/the-future-of-maritime-cybersecurity/

https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

https://www.classnk.or.jp/hp/pdf/activities/statutory/ism/flag/marshall/ism_marshall_mg-2-11-16.pdf

https://insb.gr/sites/default/files/ISM_TN_24-2017_Cyber_risk_management_into_the_ISM_Code.pdf

https://www.linkedin.com/pulse/4-cases-cyber-security-failures-shipping-history-chronis-kapalidis

https://www.utu.fi/en/sites/hazard/publications/Documents/HAZARD%20Publication%203%20CYBERSECURITY%20IN%20PORTS.pdf

https://timreview.ca/sites/default/files/Issue_PDF/TIMReview_April2015.pdf#page=35

https://apps.dtic.mil/dtic/tr/fulltext/u2/a595134.pdf

https://apps.dtic.mil/dtic/tr/fulltext/u2/a595134.pdf

http://www.imo.org/en/_layouts/15/osssearchresults.aspx?u=http%3A%2F%2Fwww%2Eimo%2Eorg%2Fen&k=cyber%20security

http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/IMO%20and%20Maritime%20Security%20-%20Historic%20Background.pdf

http://www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx

https://en.wikipedia.org/wiki/International_Maritime_Organization#cite_note-about-1

https://securestatecyber.com/cyberbloggen-en/the-future-of-maritime-cybersecurity/

https://safety4sea.com/bimco-to-launch-new-cyber-security-clause/

https://www.rivieramm.com/news-content-hub/bimco-sets-2019-target-for-cyber-security-clause-22580

https://www.bimco.org/news/priority-news/20190522-new-cyber-security-clause-from-bimco

https://www.bimco.org/contracts-and-clauses/bimco-clauses/cyber-security-clause-2019

http://www.nepia.com/insights/industry-news/new-cyber-security-clause-from-bimco/

https://britanniapandi.com/bimco-cyber-security-clause-2019/

https://www.dnvgl.com/news/dnv-gl-releases-first-cyber-security-class-notations--122642

https://www.dnvgl.com/services/maritime-cyber-security-services-and-solutions-73927#

https://www.dnvgl.com/energy/details/smart-energy/services/cyber-security.html

https://www.dnvgl.com/maritime/cyber-security-self-assessment.html

https://www.dnvgl.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html

https://www.dnvgl.com/maritime/webinars-and-videos/videos/cyber-security-awareness.html

https://www.dnvgl.com/services/information-and-cyber-security-2636

http://www.gard.no/Content/21865536/DNVGL-RP-0496.pdf

https://ww2.eagle.org/en/about-us.html

https://ww2.eagle.org/en/about-us/safety.html

https://www.maritime-executive.com/corporate/abs-launches-new-maritime-cybersecurity-risk-assessment-platform

https://ww2.eagle.org/content/dam/eagle/publications/cutsheets/maritime-and-offshore-cyber-security-abs-advanced-solutions-cutsheet.pdf

https://ww2.eagle.org/en/news/press-room/abs-confirmed-global-leader-maritime-cyber-security-seatrade-awards.html

https://ww2.eagle.org/en/Products-and-Services/advanced-solutions.html

https://ww2.eagle.org/en/news/press-room/securitygate-cyber-risk-analysis.html

https://ww2.eagle.org/en/news/press-room/cyber-security-standard-for-new-vessels.html

https://ww2.eagle.org/en/news/events-calendar/Webinar-Cyber-Security-US-Ports-Terminals.html

https://www.abs-group.com/Knowledge-Center/Project-Profiles/Cybersecurity-Analyzing-Marine-Related-Cyber-Risk-in-Critical-Systems/

https://www.maritime-executive.com/corporate/abs-launches-new-maritime-cybersecurity-risk-assessment-platform

https://ww2.eagle.org/en/news/press-room/advanced-solutions-and-fleet-management-limited-partner-on-cyber-security.html

https://www.seatrademaritimeevents.com/seatrade-awards/2019-winners

https://ww2.eagle.org/en/news/press-room/cyber-security-standard-for-new-vessels.html

https://ww2.eagle.org/en/news/press-room/advanced-solutions-and-fleet-management-limited-partner-on-cyber-security.html

https://www.lr.org/en/bimco-guidelines/

https://iumi.com/search?t=cyber+security

https://www.lr.org/en/cyber-security/

https://www.lr.org/en/latest-news/preparing-for-the-maritime-cyber-security-challenge/

https://iccwbo.org/global-issues-trends/digital-growth/cybersecurity/

https://iccwbo.org/publication/icc-cyber-security-guide-for-business/

http://www2.hgk.hr/icc/datoteke/ICC-Cyber-Security-Guide-for-Business.pdf

https://iccwbo.org/resources-for-business/incoterms-rules/incoterms-2020/

http://www2.ggori.com/incoterms-2020-what-to-expect/

https://iccwbo.org/resources-for-business/incoterms-rules/incoterms-rules-history/

https://incodocs.com/blog/incoterms-2020/

https://safety4sea.com/cm-cyber-risks-insurance-cover-and-cyber-preparedness/

https://www.linkedin.com/pulse/vessels-hackers-insurance-seaworthiness-risk-ngozi-medani

http://www.aida.org.uk/pdf/Cyber%20Risks%20and%20Marine%20Insurance%20-%20Seaworthiness,%20Causation,%20and%20Lessons%20from%20Maritime%20Piracy.pdf

http://www.giureta.unipa.it/phpfusion/images/articles/2017/05_Franchina_DirNav_13062017.pdf

https://scholar.google.com/scholar?hl=el&as_sdt=0%2C5&q=cyber+seaworthiness&btnG=&oq=cyber+seaworthi

https://books.google.gr/books?hl=el&lr=&id=UfedDwAAQBAJ&oi=fnd&pg=PA87&dq=cyber+seaworthiness&ots=CYFF8KqMa9&sig=18S6pi4rYuPFKnVXqF-kAmCffzE&redir_esc=y#v=onepage&q=cyber%20seaworthiness&f=false

https://ieeexplore.ieee.org/abstract/document/1281252

https://pdfs.semanticscholar.org/92eb/793555d584e7613d52d703c5d0b7cffb13d2.pdf

https://eugdpr.org/the-regulation/

https://www.tradewindsnews.com/safety/maritime-braces-for-the-next-cyber-breach/2-1-437319

https://www.tamimi.com/law-update-articles/a-shipowners-duty-to-provide-a-seaworthy-ship-under-the-charterparty/

http://www.ja-sr.sk/files/remediesCases.pdf

http://discovery.ucl.ac.uk/6988/1/6988.pdf

http://www.nepia.com/insights/industry-news/who-has-to-produce-the-evidence-in-a-cargo-claim/

http://www.misdevelopment.com/products.cfm?mgn

https://scortel.com/en/system-solutions/marine-information-systems

http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Default.aspx

https://www.asket.co.uk/single-post/2019/06/17/IMO-GISIS-Piracy-and-Armed-Robbery-Report---marsec-piracy

https://securestatecyber.com/cyberbloggen-en/the-future-of-maritime-cybersecurity/

https://securestatecyber.com/uncategorized/den-nya-sakerhetsskyddslagen-1-april-2019/

https://securestatecyber.com/uncategorized/why-information-security-is-important-5-common-threats/

https://safety4sea.com/cm-maritime-cyber-security-a-widening-net/

https://gcaptain.com/editorial-readying-for-the-maritime-attacks-of-the-future/

https://web.archive.org/web/20140223153859/http://www.cospas-sarsat.org/index.php
https://www.sarsat.noaa.gov/satellites1.html
https://www.cospas-sarsat.int/en/system-overview/cospas-sarsat-system
https://www.cospas-sarsat.int/images/stories/SystemDocs/Current/SD42-DEC16.pdf
https://www.oroliamaritime.com/solutions/emergency-readiness-response/
https://www.inmarsat.com/about-us/
https://iccwbo.org/content/uploads/sites/3/2018/10/the-legal-status-of-e-bills-of-lading-oct2018.pdf

https://www.maritime-executive.com/article/humans-bigger-cyber-security-risk-than-unmanned-ships

https://www.researchgate.net/publication/325195302_Cyber-Risk_Assessment_for_Autonomous_Ships

https://ieeexplore.ieee.org/document/8726823

https://safety4sea.com/cyber-liability-issues-hindering-unmanned-ships-says-new-report/

https://www.freightwaves.com/news/the-future-of-autonomous-ships-rests-in-their-ability-to-tackle-cyberattacks

http://forums.capitallink.com/shipping/2017cyprus/ppt/ioannides.pdf

https://www.hstoday.us/subject-matter-areas/maritime-security/the-future-of-autonomous-ships-rests-in-their-ability-to-tackle-cyberattacks/

https://www.ukpandi.com/fileadmin/uploads/uk-pi/Documents/2017/Legal_Briefing_e_bill_of_Lading_WEB.pdf

https://www.bimco.org/contracts-and-clauses/bimco-clauses/electronic-bills-of-lading-clause-2014

https://www.bimco.org/contracts-and-clauses/chartering-help-and-advice/bills-of-lading-advice/electronic_bills_of_lading

https://www.nortonrosefulbright.com/en/knowledge/publications/b20094b6/e-bills-of-lading

http://www.unmanned-ship.org/munin/wp-content/uploads/2012/08/R%C3%B8dseth-Burmeister-2012-Developments-toward-the-unmanned-ship.pdf

http://publications.lib.chalmers.se/records/fulltext/198207/local_198207.pdf

http://www.transnav.eu/Article_Risk_Assessment_for_an_Unmanned_R%C3%B8dseth,35,593.html

http://www.ericvanhooydonk.be/media/54f3185ce9304.pdf

ttps://pdfs.semanticscholar.org/92eb/793555d584e7613d52d703c5d0b7cffb13d2.pdf

https://knect365.com/shipping/article/c8448580-26fd-42c4-bf79-ae106655e94d/navigation-and-autonomy-the-biggest-stories-of-2019-part-2

https://www.shipownersclub.com/unmanned-autonomous-vessels-legal-implications-pi-perspective/

http://www.unmanned-ship.org/munin/about/the-autonomus-ship/

https://svw.no/contentassets/f424f309bd304e99b39f11355e98571f/svw_maritime-law-in-the-wake-of-the-unmanned-vessel.pdf

https://whatis.techtarget.com/definition/autonomous-ship

http://www.unmanned-ship.org/munin/wp-content/uploads/2016/02/MUNIN-final-brochure.pdf

https://www.bureauveritas.jp/news/pdf/641-NI_2017-12.pdf

https://marine-offshore.bureauveritas.com/sites/g/files/zypfnx136/files/media/document/%231131_BV_4PagesMARINE_BD_1.pdf

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

https://www.secureworks.com/resources/wp-what-gdpr-means-for-your-security-strategy

https://www.ncsc.gov.uk/information/GDPR

https://www.financierworldwide.com/europes-general-data-protection-regulation-from-a-cyber-security-perspective#.XY3FZFUzaHs

https://timreview.ca/sites/default/files/Issue_PDF/TIMReview_April2015.pdf#page=35