Cyber-attacks: a digital threat reality affecting the maritime industry

David Miranda Silgado

Follow this and additional works at: https://commons.wmu.se/all_dissertations

Part of the Transportation Commons

Recommended Citation
https://commons.wmu.se/all_dissertations/663

This Dissertation is brought to you courtesy of Maritime Commons. Open Access items may be downloaded for non-commercial, fair use academic purposes. No items may be hosted on another server or web site without express written permission from the World Maritime University. For more information, please contact library@wmu.se.
WORLD MARITIME UNIVERSITY
Malmö, Sweden

CYBER-ATTACKS; A DIGITAL THREAT REALITY AFFECTING THE MARITIME INDUSTRY

By

DAVID MIRANDA SILGADO
Republic of Panamá

A dissertation submitted to the World Maritime University in partial fulfilment of the requirements for the award of the degree of

MASTER OF SCIENCE
In
MARITIME AFFAIRS
(MARITIME SAFETY AND ENVIRONMENTAL ADMINISTRATION)

2018

© Copyright David Miranda Silgado, 2018
DECLARATION

I certify that all the material in this dissertation that is not my own work has been identified, and that no material is included for which a degree has previously been conferred on me.

The contents of this dissertation reflect my own personal views, and are not necessarily endorsed by the University.

(Signature):

David Miranda Silgado (Ing.)

(Date): 18th September 2018

Supervised by: Dimitrios Dalaklis, PhD
Associate Professor
World Maritime University

Supervisor’s affiliation:
Maritime Safety and Environmental Administration
ACKNOWLEDGEMENTS

Firstly, I wish to thank God, my creator, for all the blessing that given in my life, the courage to follow my goals and the strength to believe in my dreams.

I would like also to express my gratitude to the Institute for Training and Development of Human Resources (IFARHU) my sponsor, for contribute with the improvement of the Panamanian human resources, and to the Panama Maritime Authority (AMP) for supporting the professional growth of its collaborators.

I am also gracefully to my supervisor Professor Dimitrios Dalaklis for his guidance and support throughout this research project, to Professor Raphael Baumler for his constantly assistance and collaboration, and to all World Maritime University Staff, that in one way or another contributed to my performance and the knowledge gained during this MSc program.

Finally, I would like to thanks to my family that encouraged and believed in me, and my close friends that support me during all this period. All of you helped me to focus on my goals and work hard to conclude this gratifying and enriching process.
ABSTRACT

Title of Dissertation: Cyber-Attacks; A Digital Threat Reality Affecting The Maritime Industry

Degree: Mater of Science

In recent decades, technology has developed impressively; the maritime industry sector is one user of numerous new systems/equipment. This technological advance represents a considerable advantage in terms of commercial, operational and financial benefit; on the other hand, it also poses a significant risk for the security of the operations involved, highlighting that the use of the new technological systems and equipment brings to the table a series of threats that are affecting the maritime industry.

The importance of cybersecurity issues has been recognized up to a certain extent in recent years. This research presents the most significant cases of cyber-attacks in the maritime industry since 2011, covering vessels, ports, shipping companies and maritime administrations’ systems. It shows that the maritime industry is neither immune to cyber-attacks nor completely prepared to combat the risks involved in using modern digital systems. Such risks, if realized, can jeopardize the information, data and systems involved. Nevertheless, confidentiality, integrity and availability are imperative for vessel security operations, but also for shipping companies, ports and maritime administration operations due to the enormous amount of sensitive information and money that is involved in each activity.

This research effort also includes an overview of the current mitigation guidance developed by International Maritime Organization and the maritime industry with a review of the existing practices implemented by shipping companies and flag administrations. Possible consequences and cyber-attacks in terms of safety, environment and economy are discussed. Finally, conclusions and recommendations are presented, highlighting the necessity for stakeholders in the maritime industry to be aware of the current cybersecurity situations, and develop pertinent strategies to address cybersecurity issues and the use of modern system.

KEYWORDS: Cybersecurity, Cyberattacks, Safety, Security, Threats, Risks, Vulnerability, Consequences.
6.1 Discussion of Findings ........................................................................................................ 60
6.2 Conclusions ...................................................................................................................... 61
6.3 Limitations ....................................................................................................................... 62
6.4 Recommendations ........................................................................................................... 62
   6.4.1 Promote Cybersecurity Policy and Procedures ....................................................... 63
   6.4.2 Promote a Cybersecurity Risk Aware Culture ....................................................... 63
   6.4.3 Promote Sharing Information among Maritime Industry ....................................... 64
   6.4.4 Promote Tailored Training And Awareness. ......................................................... 64

VII. REFERENCES .................................................................................................................. 66

APPENDIX SECTION ........................................................................................................... 73
   Appendix 1: Definitions .................................................................................................... 73
   Appendix 2: Electronic magazine survey ........................................................................... 75
   Appendix 3: Electronic Magazine Collection of Data ....................................................... 80
LIST OF TABLES

Table 1 Classification of Cyber Threats in Shipping.......................................................... 13
Table 2 Cyber Attacks Cases............................................................................................31
Table 3 Shipping Companies and Flag Administration Questionnaire Information .... 34
LIST OF FIGURES

Figure 1. Evolution of Cyber and Physical Threats. Source: Deloitte ................................. 3
Figure 2. Scope of Study. Source: Author ............................................................................ 5
Figure 3. Classification of Threats. Source: Author............................................................. 10
Figure 4. CIA Triad. Source: Modified from Inmarsat. ....................................................... 14
Figure 5. Electronic System and Equipment onboard Vessels. Source: HudsonAnalytix. Inc. .... 17
Figure 6. ECDIS & ARPA / RADAR. Source: Electro Technical Office ............................ 18
Figure 7. IACS Recommendations. Source: BIMCO .......................................................... 23
Figure 8. Electronic Magazine Survey Result. Source: Author ........................................... 29
Figure 9. System onboard vessel and connection to shore. Source: DNV GL ...................... 53
Figure 10. Recommendations. Source: Author ................................................................. 62
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABS</td>
<td>American Bureau of Shipping</td>
</tr>
<tr>
<td>AIS</td>
<td>Automatic Identification System</td>
</tr>
<tr>
<td>ARPA</td>
<td>Automatic Radar Plotting Aid</td>
</tr>
<tr>
<td>BIMCO</td>
<td>Baltic and International Maritime Council</td>
</tr>
<tr>
<td>CIA triad</td>
<td>Confidentially, Integrity and Availability Triad</td>
</tr>
<tr>
<td>DNV GL</td>
<td>Det Norske Veritas and Germanischer Lloyd</td>
</tr>
<tr>
<td>ECDIS</td>
<td>Electronic Chart Display and Information system</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>HIMSS</td>
<td>Healthcare Information and Management Systems Society</td>
</tr>
<tr>
<td>IACS</td>
<td>International Association of Classification Societies</td>
</tr>
<tr>
<td>IMO</td>
<td>International Maritime Organization</td>
</tr>
<tr>
<td>IRISL</td>
<td>Islamic Republic of Iran Shipping Lines</td>
</tr>
<tr>
<td>ISM Code</td>
<td>International Safety Management Code</td>
</tr>
<tr>
<td>ISPS</td>
<td>International Ship Port Facility Security Code</td>
</tr>
<tr>
<td>IT</td>
<td>information technology</td>
</tr>
<tr>
<td>MODU</td>
<td>Mobile Offshore Drilling Unit</td>
</tr>
<tr>
<td>NAVTEX</td>
<td>Navigational Telex</td>
</tr>
<tr>
<td>OT</td>
<td>operational technology</td>
</tr>
<tr>
<td>RADAR</td>
<td>Radio Direction and Ranging</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>SOLAS</td>
<td>International Convention for the Safety of Life at Sea</td>
</tr>
<tr>
<td>STCW</td>
<td>International Convention on Standards of Training, Certification and Watchkeeping</td>
</tr>
<tr>
<td>TEU</td>
<td>Twenty-foot Equivalent Unit</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>VDR</td>
<td>Voyage Data Recorder</td>
</tr>
</tbody>
</table>
I. INTRODUCTION

1.1 Background

The world is relying more on technology than ever before. Numerous applications of technology have become a fundamental part of shipping, providing real information and effective communication around the world, instantaneously. Digital technology has advanced and increased exponentially in recent years; information technology (IT) and operational technology (OT) are more frequently connected to the world wide web than ever before, and the shipping industry cannot escape this reality (IMO, 2018). However, technology is also bringing along certain risks regarding safety and security of shipping operations that could possibly spill over to the economic domain, considering that both information technology and operational technology are essential for the daily operation and the sustainability of the shipping industry. The fact that more than 90 per cent of world trade is carried by the shipping industry demonstrates that the industry is a critical factor in the world economy, where intermodal freight transportation and integrated systems play an essential role. At the same time, these systems are very vulnerable to cyber-attacks (Saul, 2017).

The risk of cyber-attacks expanded exponentially at the end of the twentieth century, with the arrival of the Internet, the use of computer networks systems and the emergence of cyberspace as the basis of business. Cyber-attacks refer to the deliberate exploitation of computer systems using malicious code to disturb computers and data. Cyber-pirates, hackers, cyber-criminals, hacktivists and industrial competitors, motivated by monetary
or other benefits, obtain access and control of a targets’ system to cause damage for criminal or terrorist purposes. As already pointed out, accessing delicate systems and using maritime transportation for unscrupulous acts can compromise the safety and security of shipping operations (DiRenzo, 2017).

Digitalization is the conversion to digital technology of everything that is used in everyday life, and the use of this technology is currently a point of discussion. The investment and improvement that the maritime sector has experienced in the last decade are incredible, revolutionizing transportation and creating numerous business opportunities. Many companies, such as Maersk and IBM are on the way to commercialising blockchain technology to expand on the digital global trade platform (Maersk, 2018). Google and Rolls Royce are studying and carrying out projects on autonomous shipping and intelligent systems (Rolls-Royce, 2017). Det Norske Veritas and Germanischer Lloyd (DNV GL) and Kongsberg are promoting the introduction of a digital platform for type approval programme on cybersecurity (Kongsberg, 2017) and Inmarsat is continually expanding the security services it provides (Inmarsat, 2017). Concerning the vessel operational perspective, technology can help to maintain safe navigation, reduction of manning, as well as secure and effective vessel operations.

The fourth industrial revolution brings to the stage, more means exposed to cyber-attacks, than ever before, raising cyber risks in term of connectivity (see figure 1). Nonetheless, in the interconnected shipping industry, where new technology applications and digital systems are continually evolving, the operational time and effectiveness of each process is essential for business transactions. It is necessary to point out that the development of cybersecurity measures goes hand in hand with advancements in technology. However, there is still a lack of understanding related to complex cybersecurity issues and the future challenges that companies will face concerning cyber-attacks. It is indispensable to consider that the human factor plays a fundamental role in the effectiveness of the attacks as a significant vulnerability element for companies. According to a maritime survey
carried out in 2016 by HIS Fairplay in association with Baltic and International Maritime Council (BIMCO), malware represents 77 percent of all maritime cyber-attacks (Di Rollo, 2017). Therefore, developing cyber security policies and implementing multi-level security strategies to address cyber threats and risk, along with prioritizing internal action and increasing cybersecurity culture to promote security awareness and training of human resources will be vital for a company’s safe operations.

![Evolution of Cyber and Physical Threats](image.png)

*Figure 1. Evolution of Cyber and Physical Threats. Source: Deloitte*

The growth of digitalization and the connectedness produce pressure on the industry to be more and more connected. Nonetheless, the absolute dependency of systems and equipment regarding interconnectivity operations is creating more vulnerability and representing an increase in opportunities for the cyber-criminal (NEP&I, 2017). A report by Juniper research indicates that cybercrime will become a $2.1 trillion issue by 2019. All the facets of the maritime industry will be impacted, including ocean container...
shipping, logistics, ports and related businesses, showing that in such a multifaceted environment, there is a necessity for global action. For that reason this dissertation examines the current cyber security situation in the maritime industry. It examines the most significant cyber-attacks cases in the last seven years along with their consequences, with the purpose of recommending that companies take into consideration the necessary preventive actions required. Moreover, it reviews recent industry guidelines, and proposes the creation of a cyber-security training and awareness program, with the objective of reducing the consequences of future cyber-attacks.

1.2 Aim

The aim of this research is to compile all information available from open sources related to cyber-attack cases in the maritime industry. This information is used to produce a timetable of past cases along with a critical evaluation and analysis of the systems involved, means of entry and consequences of each case, with the aim of increasing awareness and carrying out risk analysis. A theoretical and literature review demonstrates the exposure, vulnerabilities and possible consequences in terms of safety, environmental and economic risk to the maritime sector. Furthermore, the current framework of cybersecurity measures introduced in the maritime industry is discussed. Finally, expert opinion is used to discuss and conclude, highlighting the importance of the cyber-attack issue affecting the maritime industry.

1.3 Objectives

1.3.1 Create a list of recent cyber-attacks cases with detailed information, through a collection of reports, mainly from maritime electronic journals, magazines and articles, showing the specific areas affected and the consequences of the cyber-attacks, to demonstrate the importance of the cyber-security measures to the maritime industry.
1.3.2 Collate data from questionnaires sent to flag administrations and ship owners, to carry out a critical analysis of the current action taken against cyber-attacks, making evident the relevance of the cyber-security system in the maritime industry and the need for new regulations and effective implementation regarding cyber security policy.

1.4 Scope of study and structure

The maritime transportation industry is a sector that, in terms of network and connectivity, has long-range but, at the same time, many stakeholders are involved in the development of the different processes. Therefore, the scope of this study is specifically limited to shipping companies, port, maritime administration and ship systems (see figure 2), with a classification of intentional direct and non-intentional direct, as a means of hazards for the shipping systems in terms of cyber security.

Figure 2. Scope of Study. Source: Author
The analysis of cyber-attacks in the last seven years will make available a general overview of the real situation of cybersecurity issues, and the current guidance and shipping industry practice will provide sustenance for possible recommendations that need to be taken into consideration to address this risk.

The structure of this dissertation includes six chapters:

Chapter I provides the introduction with background information, aim, objective, dissertation structure and scope of the study, as well as the various relevant definitions.

Chapter II establishes a theoretical and literature review, which focuses on historical background, exposure, vulnerability of technology systems supporting the maritime industry and possible consequences of cyber-attacks in terms of safety, environment and economy.

Chapter III demonstrates the investigation development, including the research methodology, risk analysis, research questionnaire and hypothesis used in this research.

Chapter IV presents an assessment of the present cybersecurity measures using data from past cybersecurity attacks and a risk analysis.

Chapter V reveals the cybersecurity mitigation practices through a summary of different guidelines provided by the IMO and the maritime industry; it also presents a risk mitigation analysis, evaluation of the actions and preventive measures taken by Flag Administration and shipping companies, while carrying out a comparison of the data collected from the questionnaire. Finally, it discusses the barriers to cyber security implementation, which include cost, company policy, training, control and monitoring, and enforcement by flag, coastal and port states.

Chapter VI summarizes the findings, and presents the conclusions, limitations and recommendations obtained via this research.
1.5 Definitions

Considering the complexity and different approaches in the terminology used to discuss cyber security issues, a rigid framework of analysis is needed. Below, a list of the essential terms and words used in the current research effort is provided. However, a more detailed list of terms and definitions is attached in the annexes section.

I. Cyber incident: is an occurrence, which actually or potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences (BIMCO, 2016).

II. Cyberattacks: Any type of offensive manoeuver that targets IT and OT systems, computer networks, and/or personal computer devices attempting to compromise, destroy or access company and ship systems and data (BIMCO, 2016).

III. Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. (ABS, 2016).

IV. Hazard: Source, situation or act with a potential for harm, in terms of injury or ill health, damage to property, damage to workplace environment or a combination of these (ABS, 2016).

V. Malware: is a generic term for a variety of malicious software which can infect computer systems and impact on their performance (BIMCO, 2016).

VI. Risk: According to Oxford dictionaries risk is defined as a situation involving exposure to danger, with the possibility that something unpleasant or unwelcome will happen (Oxford dictionaries, 2018).
VII. Virus: is a hidden, self-replicating section of computer software that maliciously infects and manipulates the operation of a computer program or system (BIMCO, 2016).

VIII. Vulnerability: A weakness of an asset, or group of assets, that can be exploited by one or more threats (IET, 2016).

IX. Information technology: Information Technology (IT) is a business sector that deals with computing, including hardware, software, telecommunications and generally anything involved in the transmittal of information or the systems that facilitate communication (Techopedia, 2018).

X. Operational technology: includes devices, sensors, software and associated networking that monitor and control onboard systems (BIMCO, 2016).
II. ANALYSIS OF CYBER SECURITY THREATS.

2.1 Historical Background

Throughout history, the seas and the oceans have been associated with danger and insecurity, as a consequence of geopolitical dispute and piracy attacks. For that reason, issues of maritime security have become a concern among the stakeholders involved in the maritime sector. The International Maritime Organization agenda has reflected these concerns in recent years with certain regulatory initiatives. Over time, the panorama has been modified, but the threat remains; a “new generation” of criminal has exchanged weapons for computers, making cyber-attack the new security threat worldwide.

The complexity of the systems and the stakeholders involved in the maritime operation necessitate that every company consider the threats from different perspectives, according to the service provided and the vulnerabilities of the system. Nevertheless, the threats presented in the maritime industry can be classified into two main elements: the intentional direct threats and the un-intentional direct threats (see figure 3).
The intentional direct can be attributed to:

- **Hacktivism or activist group:** These groups are formed by ideologically motivated individuals, for which the main action is an online protest with the aim of accessing the system, and stealing sensitive information and data to use for a malicious purpose (IET, 2016).

- **Espionage industrial competitor:** They are organized to perform acts of espionage with the main objective of obtaining access to confidential information, destroying data and stealing intellectual property in order to use them for competitive advantage or to disrupt business operations (IET, 2016).

- **Government-driven or state sponsored:** There is a recognition in the maritime industry that many countries are involved in cyber-attacks (see chapter 4). Their purpose is to obtain access to state secrets, highly sensitive information, commercial information and valuable documents, to be used with the intention of...
directly affecting another state or institution of high importance to a nation, and with this act create national destabilization or chaos, or gain an economic advantage or information control (IET, 2016).

- **Terrorism:** Terrorist groups can use electronic and computerized media as a new modus operandi to carry out their terrorist acts against other groups, nations, and companies, gaining access and interrupting the operating system, for ideological, religious or political interests or purposes (IET, 2016).

- **Criminals:** Individuals or criminal organizations use cyber-attacks against interconnected systems and networks, with the intention to carry out criminal activities, mainly focused on fraudulent operations, extortions or theft of intellectual property. It is also recognized that these criminals, when they obtain access to the different systems, can control operating systems to facilitate the trafficking of drugs, arms and contraband money to obtain economic benefits or to sell valuable information to another (IET, 2016).

**Un-intentional direct are related to:**

- **Internal threat or Nature:** These can be employee or service provider mistakes. Internal employees can compromise the maritime industry systems by way of negligence, carelessness, ignorance or just human error, by accidentally opening malicious emails, using infected removable media, or accessing false websites and social media. These unintentional acts expose sensitive systems or data to threats, putting the security of companies at different levels of risk depending on the access they have to systems (IET, 2016). It is recognized that this type of threat represents a lack of training and awareness of the employees and poses the maximum risk for companies. Additionally, “by nature” can be described as an error in a system, software or application stemming from bad installation or
manufacture, which does not provide the security measures necessary to keep the system safe. (NEP&I, 2016).

Table 1 demonstrates a number of the most significant threats identified within the maritime industry and classified as Intentional Direct and Un-intentional Direct with their objective, motivation and target. Each threat presented in this table represents a high risk for the industry in different aspects. Some are more directly focused on personal economic benefit; others are more related to competition and business interests. A few of them are connected to ideological content, and ending with human error, as key factor which is attributed to many maritime accident.

The examples of threats presented in Table 1 demonstrate that actors involved in cyber-attacks incidents have well identified their targets in the shipping industry, and that the technological advances create more opportunities for criminal organizations or individuals to successfully perform cyberattacks.
<table>
<thead>
<tr>
<th>Threats</th>
<th>Intentional Direct Actors</th>
<th>Un-intentional Direct Actors</th>
<th>Objectives</th>
<th>Motivation</th>
<th>Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacktivism</td>
<td>Activist</td>
<td>N/A</td>
<td>Destruction of Data</td>
<td>Egoism / self-proclaimed</td>
<td>Governments</td>
</tr>
<tr>
<td></td>
<td>Disgruntled employees</td>
<td></td>
<td>Publication of sensitive data</td>
<td>The challenge</td>
<td>Organization</td>
</tr>
<tr>
<td></td>
<td>Individual</td>
<td></td>
<td>Media Attention</td>
<td>Political change</td>
<td>Individuals</td>
</tr>
<tr>
<td></td>
<td>Organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Governments</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Espionage or Industrial</td>
<td>Nations</td>
<td>N/A</td>
<td>Stealing data</td>
<td>Commercial espionage</td>
<td>Governments</td>
</tr>
<tr>
<td>competitors</td>
<td>Organizations</td>
<td></td>
<td>Selling stolen data</td>
<td>Industrial Espionage</td>
<td>Organization</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Ransoming stolen data</td>
<td>Intellectual property</td>
<td>Individuals</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Ransoming system operability</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Information advantage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governments driven or State</td>
<td>Nations</td>
<td>N/A</td>
<td>Gain Knowledge</td>
<td>Political gain</td>
<td>Governments</td>
</tr>
<tr>
<td>sponsored</td>
<td>Organizations</td>
<td></td>
<td>Stole sensitive data</td>
<td>Espionage</td>
<td>Organization</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Manipulation</td>
<td></td>
<td>Individuals</td>
</tr>
<tr>
<td>Terrorism</td>
<td>Terrorists group</td>
<td>N/A</td>
<td>Disruption to Economies and critical national</td>
<td>Political change</td>
<td>Governments</td>
</tr>
<tr>
<td></td>
<td>Nations</td>
<td></td>
<td>structure</td>
<td>Fear</td>
<td>Infrastructure</td>
</tr>
<tr>
<td></td>
<td>Individual hackers</td>
<td></td>
<td></td>
<td>Political, religious and ideological</td>
<td>Public targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>goals</td>
<td>Organization</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Individuals</td>
</tr>
<tr>
<td>Criminals</td>
<td>Criminal Organization</td>
<td>N/A</td>
<td>Arrange fraudulent transportation of cargo</td>
<td>Financial gain</td>
<td>Organization</td>
</tr>
<tr>
<td></td>
<td>Individual</td>
<td></td>
<td>Compromise data and network</td>
<td></td>
<td>Individuals</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Information advantage</td>
<td></td>
<td>Various types of assets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Trafficking / Smuggling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal threat or Nature</td>
<td>N/A</td>
<td>Employee</td>
<td></td>
<td></td>
<td>Poor operational design</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Workers</td>
<td></td>
<td></td>
<td>Technical or physical failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manufacturers</td>
<td></td>
<td></td>
<td>Failure on Process and implementations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service Provider</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Author
2.2 Exposure

The exposure that characterizes the computerized system and its interconnectivity opens up the door to smart attackers to perform their criminal acts, considering that the business in the maritime sector has a very high profile with notable revenue. Unfortunately, the consequence can be devastating (Marsh & McLennan, 2014). The most important security goal of the Internet of Things is to ensure that security mechanisms used in the system can properly ensure security of the data and system, using the three components of the CIA triad (Confidentiality, Integrity and Availability) (see figure 4). Confidentiality of the data represents the use of sensitive and confidential information by authorized personnel only, and provides the security mechanisms to maintain the privacy of the data and system. The Integrity mentioned in the CIA triad refers to the protection of valuable information and data from external and internal actors during daily system use. Moreover, Availability permits immediate access of authorized personnel to information and data for normal operation or in dangerous situations, providing independence for the company in terms of using their resources. Nevertheless, a break on one of these elements can result in serious damage to the company security system, affecting the company operations and exposing the systems involved (Farroq, Wasseem, Khairi & Mazhar, 2015).

![CIA Triad Diagram](image)

*Figure 4. CIA Triad. Source: Modified from Inmarsat.*
2.2.1 Companies

The exchange of information and data across many stakeholders involved in shipping companies operations draws the attention of cybercriminals to performed attacks, inasmuch as each system has different cybersecurity measures. Many systems are involved in the process of handling valuable information, data and code. Bank transferences and money movements are incentives for criminals. The most common method is the use of ransomware, where the attacker encrypts the system (computer or database), and requests the victim to pay a ransom to get the data back. This is very comparable to piracy attacks where the criminal physically hijacks the vessel, crew and cargo until someone pays a ransom, which in the history of Piracy attacks, has been a successful business modus operandi. It is evident that the exposure in shipping companies is reflected directly in the system, database and, operational and internal procedures, which represent a valuable asset for the companies.

2.2.2 Ports

For the port operation, the main component is cargo handling; the includes the tracking, transporting and inspecting system of the cargo until it is received by the retails, the un-loading and loading system, which manipulated the cargo, and the crane operation for distribution and movement of cargo. All of these modern systems and equipment now use technology and network connections to carry out daily operations, making the exposure of the port evident (DiRenzo, 2015). For example, the system used for movement of cargo can be used for drug smuggling, weapon trafficking and other criminal acts. The control of the cargo operation gives the criminal the facility to move cargo without authorization.
2.2.3 Administrations

The data handled by the Maritime Administration contains a large amount of detailed information, valuable to various maritime stakeholders. The system used by the maritime administration can be exposed to cyber espionage by other states, whose aim is to obtain access to sensitive data that can be used for their own purposes. Furthermore, ransom that can be obtained is another motivation for these criminals. However, the maritime administration also presents internal exposure with its large number of the employees, who have access to critical systems and are interconnected with the network, increasing exposure for the administration and the risk of being cyber attacked.

2.2.4 Ships

Exposure on modern ships has increased tremendously in recent years because of their dependency on sophisticated electronic means like AIS (Automatic Identification System), ECDIS (Electronic Chart Display and Information system), GPS (Global Positioning System), VDR (Voyage Data Recorder), Radar/ARPA (Radio Direction and Ranging)(Automatic Radar Plotting Aid), GMDSS (Global Maritime Distress and Safety System), and other advanced system used and connected for the crew to vessel network system (see figure 5). All of these result in significant danger to the safety of the vessel’s operation, which due to its interconnectivity and recurrent use, is open to cyber-attacks (DiRenzo, 2015).
AIS, since 2002, has been mandatory for all passenger and sea-going vessels with 300 gross tonnage or more. It is a tool for vessel safety, collision avoidance and ship's monitoring, providing vessel information and status. Course, speed, and position are some of the information displayed in the AIS for the safety and security of vessel operation. However, the exposure of the AIS, concerning connectivity and information provider, represents a high risk for vessel operation. If the AIS it is cyber attacked, the consequences in terms of communication interconnectivity with ship-to-ship, ship-to-shore and shore-to-ship, can be significant (Tetreault, B. J, 2005). Furthermore, it has been proved that the AIS does not have the necessary security measure integrated, exposing it to cyber-attacks. The next chapter will present a cyber-attack case that demonstrates that it is possible to deactivate and manipulate the AIS information to create a false collision or SAR alert (Pajunen, 2017).
Another electronic means exposed to cyber-attack is the Electronic Chart Display and Information System, which in June of this year became mandatory for existing vessels as an essential aid for navigation (see figure 6). The ECDIS runs in a basic computer without an internet connection, which means that it cannot be remotely infected. However, the high risk of exposure involves the system updates process by the bridge team because the ECDIS does not have antivirus installed. This happens due to insufficient computing power, and because the antivirus does not support the operating system used, which makes the computer completely unprotected (Pajunen, N, 2017).

![ECDIS & ARPA / RADAR](image)

**Figure 6. ECDIS & ARPA / RADAR. Source: Electro Technical Office**

One of the main issues is that the bridge navigation equipment is more integrated. Some manufacturers are the providers of many items of equipment, and they make it compatible. As a consequence, the ship-owners find a practical way to buy equipment from only one manufacturer to ensure compatibility. Additionally, interconnection with the engine, remote accessibility, and poor design of software and hardware are critical factors in exposure of the vessel and satellite communication.
2.3 Vulnerability of Technological Systems

In the maritime environment, the equipment, systems and devices are rapidly increasing the connectivity to the network, which facilitates accessibility and functionality and provides more efficient operations. The connected devices include the navigational system, communication system, cargo management system, engine system, dynamic system, terminal management system, tracking system, logistic system and many more. However, the growth of the connected devices results in high risk for the maritime industry, increasing the vulnerability of all the integrated bridge, engine, cargo, communication and land systems mentioned. For that reason, it is necessary that the maritime sector evaluates the vulnerabilities in the sophisticated and interconnected systems, which are incorporated in daily operations, and understand the complexity of maritime system vulnerabilities. (Clark, 2017).

2.3.1 Companies

Shipping companies, due to the nature of the services they provide, the number of financial transactions they conduct, and the sensitivity of the information and data they handle, have become a very important sector to discuss in this research. Some the vulnerabilities that are present in these companies are the IT systems at the operational and management levels. These are involved in all the delicate company operations involving cargo movement, authorizations, inspections, records, financial transactions, security access, and human resources. Also vulnerable are the communication networks that help maintain a continuous flow in terms of sending and receiving information and data between stakeholders, including Wi-Fi, phone systems, and satellite communications (Reiskind, 2018). The lack of cyber security knowledge and awareness, the poor implementation of policies and procedures related to cyber security, and undeveloped cyber risk management are other common vulnerabilities of shipping companies (Allianz, 2016).
The list of shipping company needs to be addressed individually because each company has a different type of vulnerability depending on its services and its interconnection with others.

2.3.2 Ports

The port operation is very complex because of the nature of the services provided, the number of processes taking place in this infrastructure and the large number of workers involved in the operation, which includes land, sea and economic activities. To ensure the smooth flow of the operation, it is necessary to enhance physical and cyber security measures. The International Ship Port Facility Security Code (ISPS) presents a clear legislation on implementation and maintenance of port security measures. It includes specific procedures and designates tasks and responsibilities, such Port Security Plan, Port Security Officer and Port Facility Security Officer, covering ship and port facility operations (Chiappetta, 2017). However, contemporary worldwide port operations are profoundly connected with network management and logistics systems, including tracking, loading, unloading and transportation of cargo. This dependency and reliance on complex networked systems and interconnectivity create a significant vulnerability in the system associates in port and cargo operation, which can become a subject of cyber-attacks. (DiRenzo, 2015).

Vulnerabilities faced by ports are related to the interconnected operation of port authorities, maritime companies, customs, ministries, financial institutions, vessels, crews, cargoes, IT providers, infrastructures, and data flow that are vital for maritime trade and the world economy.
2.3.3 Administrations

A Maritime Administration has under its umbrella many areas of interest, such as vessel and seafarer certification, vessel registers, port authorities, inspections, applications, enforcement, business transactions, money transfers, national and international communication, databases, international offices, integrated systems, and network systems. All these operating systems are connected to electronic means and interconnected with each other and with the different partners and customers, which can be potentially vulnerable to cyber-attacks. For that reason, the maritime administration in addition to regulating the stakeholders involved in the services it provides, must take the appropriate measures to safeguard its own system, data and information. In addition, each administration should carry out an internal risk analysis to determine the possible vulnerability of its system to cyber-attacks and implement internal cyber security measures in terms of identifying, protecting, detecting, responding, recovering and creating a cyber-security culture (Kneeland, 2014).

2.3.4 Ships

One of the most essential systems used for the safety of navigation and operation of the ship are GPS, ECDIS and AIS. GPS, which provides vessel positioning, is indispensable to the vessel’s navigation. Jamming of the GPS can represent a substantial challenge for the safety of vessel navigation. Another important system is the Automatic Identification System, which, as a result of the cyber-attacks, can create a ghost ship that can be detected by other vessels and ports. A cyber-attack could also modify ship information details, such as course, name, cargo, position, and speed, or send false warnings, alarms and distress signals. One more system used for vessel navigation is the Electronic Chart Display and Information System, used to supplement the old-style navigation charts. It is interconnected with other vessel systems and sensors, such as Navigational Telex.
(Navtex), AIS, echo-sounder, radar, and anemometer (Clark, 2017). The exclusive reliance on electronic systems, which can be cyber-attacked, can result in danger for maritime operations, as presented in section 4.1: Different cybersecurity attack cases and their consequences.

According to cyber keel report, a satellite communication study was carried out by IOActive Security Company in 2013, using Inmarsat and Iridium Sat-Com terminals. The result of this study indicates that certain systems have severe security issues. All the devices included in the scope of the analysis could be abused and easily compromised, just as sending a message from one vessel to another; compromising satellite communication system, gives to the attackers' control of the information that passes through the satellite link. However, another vulnerability faced in terms of vessels and sat-com is the fact that crew, passengers and external persons have access to the ship, and sometimes to the equipment and systems. This situation highlights the lack of control of the IT system and the over reliability on the ship-owner’s side (Cyberkeel, 2014).

To address these vulnerabilities, it is recommended that ship owners implement the cyber guidance provided by the sector and carry out the necessary risk assessments. Additionally, they should train the crew and personnel involved in ship operations. Moreover, ships need to be build according to the International Association of Classification Societies (IACS) standards and recommendations (see figure 7), and systems and equipment should have contemporary software (Sørensen, 2018).
The examples mentioned demonstrate how fragile the interconnectivity in the maritime industry has become, showing that disruption and failure in the critical systems and equipment have caused severe impacts on maritime transportation, worldwide trade and international economies.

2.4 Possible Consequences of Cyber Attacks

The magnitude of the consequences of cyber-attacks depends on the nature of the cyber-attacks themselves, the complexity of the scenarios and the procedures already established by the industry. Following is possible descript consequences of the cyber-attacks in term of safety, environment and economic impact.
2.4.1 Safety

There are many systems, types of equipment and various technologies in the maritime industry and onboard vessels, including bridge, cargo handling, ship control access, propulsion, machinery, communication, and administrative which depend on the electronic systems (Belmont, 2016). The International Maritime Organization through The International Convention for the Safety of Life At Sea (SOLAS), Regulation V/19, 20 and 27 requires carrying onboard an AIS and ECDIS and requires having a receiver for a global navigation satellite system (GPS). However, some of the safety risks that have been reported are in navigation equipment system, such as the AIS, ECDIS, and GPS, which are essential for navigation, and vessel positioning. For that reason, jamming or disruption on any of these essential navigation systems becomes a severe problem that can affect the maritime industry (Caldwell, 2010).

2.4.2 Environment

Environmental pollution is another potential risk related to cyber-security. Every year, diesel, oil, petrol and other toxic chemicals are spilt into the sea. The majority of the accidents involve tanker vessels, barges, platforms and petroleum shore stations. The reasons for oil spills occurring include vessel collisions, groundings, oil cargo transfers, fuel tank overflows or oily water pumped from the bilge. Oil spills on the sea can have severe impacts, including damage to wildlife, habitats, and ecosystems. One case of severe environmental damage inflicted by an oil spilled is the case of M/T Exxon Valdez, in which the vessel ran aground in Prince William Sound in 1989, spilling 10.8 millions of US gallons of crude oil in Alaskan waters. It is considered one of the most dramatic and devastating accidents related to oil spills, destroying and killing thousands of mammals, fish, whales, and birds. Today evidence of persistent pollution still exists in Prince William Sound, representing significant damage to the ecosystem of the area and the residents’ health (Belmont, 2016).
There are many environmental risks in the maritime industry, such as ballast water discharge, sewage, and emission of gasses. All the equipment or apparatuses on board the vessels that regulate loading, discharge, and emissions, are controlled by electronic systems if the vessel is cyber attacked, all this equipment is vulnerable and can be used to carry out criminal acts or specific damage, signifying a potential risk to the environment and human health. Additionally, malware infections have occurred on several offshore rigs and platforms in recent years. According to the Houston Chronicle, cyber-attackers such as criminals or terrorists with knowledge of oil platforms, refineries, pipelines and technology systems can distribute malware in these structures, representing a catastrophic scenario and high level of risk to people and to the environment (Shauk, 2013).

The maritime industry must be cognizant of the probable devastating effects that cyber-attacks can have on shipping companies, vessels, ports and maritime administrations, with catastrophic environmental impacts and consequences that can result in business interruption, financial loss and reputational effects. To minimize the possible negative outcomes in terms of environmental damage, it is essential to develop and implement robust cybersecurity measures and actions (Ginter, 2010).

**2.4.3 Economic**

Information technology is one of the utmost important factors in modern business operations, if the business information and systems are not secured appropriately, the system, data and information are susceptible to cyber-attacks. As is mentioned above, the maritime industry is not immune to cyber-attacks. The data and confidential information that is handled by the maritime sector is very attractive to cyber attackers. Furthermore, particular economic risks involve business interruption, information recovery, equipment repair and system installation, which, as mentioned in this chapter, represent a great loss for the companies. In addition, the necessary actions to avoid future cyber incidents denote a considerable investment in cyber-security systems for the companies (Rose, 2017).
Today almost all companies use networks, internet and interconnected systems as a principal means for business; in fact, many companies do not even have physical offices. Everything is done online. However, all these operations and activities can be monitored and interfered with. In that event, protection from cyber-attacks is required to minimize possible economic consequences that can directly or indirectly affect individuals, organizations and society. According to Arthur J. Gallagher & Co, an insurance firm, the transportation sector is ranked third in terms of cyber vulnerability. According to the firm’s study, 2017 was a top year for cyber-attacks, with an average financial cost per average medium sized company of around $3.79 million (Gallagher, 2018).

Another relevant economic consequence resulting from cyber-attacks is the loss of intellectual property, which is one of the biggest threats to the business. Indeed, companies have been investing in cyber-security systems to prevent the loss of intellectual property. This means that many companies have suffered monetary costs investing in new systems and technology. According to Business Matters (2016), the “United Kingdom government report highlighted IP (Intellectual Properties) theft as the most damaging cyber-crime for UK businesses, resulting in a loss of £9.2bn a year”.

2.5 Concluding Thoughts

In this chapter, the different threats, exposure, vulnerability and possible consequences related to cyber security issues were discussed. It is important to understand how the threats can affect the maritime industry, other sectors, society and economy. However, depends on the service that each company provides. For that reason, it is necessary to carry out a risk assessment to understand the threat and risk level, and the exposure and vulnerability of each system and piece of equipment. Nevertheless, the commitment in this respect needs to start at management and organizational level and then filter down to the different organizational levels.
Untrained or inadequate trained personnel represent a high-risk to each shipping operation. As a consequence, the education and training of the personnel needs to be taken into consideration as a key element of the safety and security of the shipping operation. Another essential element is the use of the guidelines provided by the maritime sector. This is in relation to shipping companies. However, as other stakeholders are involved. Therefore, it is critical to keep in mind that the consequence of a cyber-attack, which can result in catastrophic consequences in terms of safety and the environment, can also cause serious commercial and economic loss. The important point here is that the industry is working hard to regulate vessels but what will happen with ports, shipping companies, maritime administrations, suppliers, vendors and many other stakeholders involved in vessel operations?.
III. RESEARCHING CYBERSECURITY EVENTS RELATED TO THE MARITIME INDUSTRY

3.1 Methodology

The method used in this research is a combination of descriptive and analytical methods, reviewing and comparing the actions implemented and preventive measures taken by shipping companies and flag administrations against cyber-attacks. Additionally, different cyber-attack cases and their consequences are discussed, making evident the impact of cyber-attacks in the maritime industry in terms of safety, environmental and economic risk.

The collection of data for this dissertation was carried out through a literature review obtained mainly from various articles, electronic magazines, publications and books from different maritime magazines, shipping companies, flag administration statements, and classifications societies’ web sites. This collection of data as primary sources is collected through an internet search and physical access.
The literature selected for review was based on a survey of 53 people, which revealed that the most well-known electronic maritime magazines are Fair Play, Digital Ship, Tradewinds and Lloyd’s List, which is presented in figure 8 respectively. All of these journals are specialize directly in the shipping industry, with a long history and prestige in the sector.

![Figure 8. Electronic Magazine Survey Result. Source: Author](image)

The literature review covers the last seven years of cybersecurity issues (2012-2018), taking into consideration the most significant cases presented to the public in this period. The total number of the papers reviewed for this research was **1,069**, including:

- **Lloyd’s List 657**
- **Digital ship 130**
- **Tradewinds 120**
- **Fair Play 18**
- **Others 144**

In which the keyword used are:

- **Cybersecurity**
- **Cyber-attacks**
- **Cyber**
- **Security**
- **Attacks**

The results showed **181** papers associated with cyber security issues as an investigated subject.
Table 2 shows the most significant cyber-attack cases compiled during the collection of data, pointing out the limitations associated with protected information, in that many companies keep attacks secret as a protective measure. Nevertheless, Table 1 presents a brief summary of the public cyberattack cases. Detailed information regarding these cases is provided in the Chapter IV, 4.1 Past cyber-attack cases.

A small classification of fact is presented, where:

- One * mean low probability of being attacked
- Two ** mean medium probability of being attacked
- Three *** mean high probability of being attacked
<table>
<thead>
<tr>
<th>Date</th>
<th>System</th>
<th>Mean of Entry</th>
<th>Name or Place</th>
<th>Consequence</th>
<th>Classification</th>
<th>Reference</th>
</tr>
</thead>
</table>
| 2011  | Shipping Company Operational System | IT system hacked    | The Islamic Republic of Iran Shipping Lines (IRISL) State Owner Iran | • Damage operational data & Internal company communication network  
• Movement of cargo without company control resulting in lost and incorrect delivery of cargo  
• Financial loss | ***            | Gliha, D. 2017  
Hayes, 2016  
Hutchins, 2015 |
| 2012  | Shipping Company Operational System | Phishing mail employee sabotage | Saudi Aramco Company Oil & Gas Operator State Owner Saudi Arabia | • Files disappear  
• Disconnected Phone Connection  
• Loss of network communication  
• Disconnection of internal network  
• 35.000 computer shutdown  
• No money transference enabled  
• Stop operations  
• Five month to restore system  
• Financial loss | ***            | Vella Heidi, 2016  
Pagliery, 2015  
Perlroth, 2012  
Reuter, 2012 |
| 2012  | Cargo & Tracking System         | IT system hacked    | The Australian Custom and Border Protection Australia Government | • Loss control of cargo systems  
• Drug smuggling transportation | *             | Meyer-Larsen Nils, 2017 |
<table>
<thead>
<tr>
<th>Date</th>
<th>System</th>
<th>Mean of Entry</th>
<th>Name or Place</th>
<th>Consequence</th>
<th>Classification</th>
<th>Reference</th>
</tr>
</thead>
</table>
| 2012  | Maritime Administration Systems             | Virus Infiltrated by Pdf Doc           | Danish Maritime Authority Denmark | • Disclosure of sensitive information  
• Propagation of the virus to other governmental institutions  
• Shutdown network system                                                                                                             | **             | • Cyberkeel, 2014  
• The local, 2014 |
| 2013  | Port Cargo & Tracking System                | Virus Infiltrated                      | Port of Antwerp Belgium        | • Control by criminal of the security access  
• Control by criminal of cargo operation  
• Drug smuggling and money laundering for 2 years                                                                                       | **             | • Clark Julian, 2017  
• Bateman, 2013  
• Bell, 2013  
• Europol, 2013  
• Digital Ship, 2014/17 |
| 2013  | Operational System                          | Malicious software download by USB with piracy virus | Oilrig & platform Houston United States of America | • Incapacitation of computers and operating systems  
• Paralysis of one oilrig  
• Loss of communication with navigational system  
• Immobilization of thruster  
• Drifting                                                                                                                              | **             | • Belmont, 2016  
• Hayes, 2016  
• Shauk, 2013 |
| 2016  | 280 Vessels GPS System                      | Jammed by hacker                       | Vessels on South Korea         | • Problems with navigational systems  
• GPS signal died  
• GPS signal false information  
• Vessels stop operation                                                                                                                | **             | • Graham, 2017  
• Saul, 2017 |
| 2017  | One container Vessel                        | Navigation system hacked               | Course of Cyprus to Djibouti    | • Loss of control of the vessel navigation for 10 hours  
• No maneuvers permitted  
• Invest of maritime security program                                                                                                      | **             | • OSM, 2018  
• Tanya Blake, 2017 |
<table>
<thead>
<tr>
<th>Date</th>
<th>System</th>
<th>Mean of Entry</th>
<th>Name or Place</th>
<th>Consequence</th>
<th>Classification</th>
<th>Reference</th>
</tr>
</thead>
</table>
| 2017  | Port System           | Not Petya Virus        | A.P. Moller-Mearsk          | • Massive disruption of systems  
 • Port operation suspended  
 • Cargo operation suspended  
 • IT system shutdown  
 • Financial loss  
 • Invest in new equipment and software | *              | Novet, 2017  
 Jon, 2018  
 Digital Ship, 2017/18  
 Fairplay, 2018  
 Tradewinds, 2018  
 Lloyd´s list 2017/18 |
| 2017  | Shipping company System | Hacked computer system | BW Group Singapore         | • Internet connection suspended  
 • Company operation affected (Ports and vessels operations, oil and gas production)  
 • Financial loss | ***            | Platts, 2017  
 Mohindru, 2017  
 Tradewinds, 2017 |
| 2017  | Shipping company System | Hacked by virus       | Clarkson Shipbroker         | • Access to the company’s computer system  
 • Criminal access to data and information system  
 • Invest in security measure | ***            | Digital Ship, 2018  
 Nadkarmi Namrata, 2017  
 Clarkson PLC, 2017  
 Tradewinds, 2018 |
| 2018  | Shipping company system | Ransomware attack     | Long Beach Terminal Cosco U.S.A. | • Criminal obtain access to the company’s computer system, sensitive data and information  
 • Shutdown network system | ***            | Tradewinds, 2018 |

Source: Author
As a secondary source of information, stakeholders, such as ship owners and flag administrations, were approached via interview, meeting, e-mail, and calls to collect information regarding previous cyber-attack issues and the implementation of preventive measures regarding cyber-security systems. Additionally, to findings were compared with those obtained from the literature review. This analysis is carry out through the answer received of the questioner send by the internet. The Table 3, shows the number of questionnaires sent, number of responses received and the total number classified in shipping companies and maritime administrations.

Table 3 Shipping Companies and Maritime Administration Questionnaire Information

<table>
<thead>
<tr>
<th>QUESTIONNAIRES TO:</th>
<th>N° OF QUESTIONNAIRES SENT</th>
<th>N° OF ANSWERS RECEIVED</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHIPPING COMPANIES</td>
<td>16</td>
<td>2</td>
</tr>
<tr>
<td>MARITIME ADMINISTRATIONS</td>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td>TOTAL</td>
<td>30</td>
<td>5</td>
</tr>
</tbody>
</table>

3.2 Risk Analysis

Maritime accidents and incidents often occur in the shipping industry because it is a global and brutally competitive environment, which can be characterized by high, fast and expanding commercial pressure, remote owners, sub-standard ships, multinational crew, accelerated technological changes and lack of compliance with mandatory regulations. For that reason, when important decisions have to be made, it is necessary to carry out a risk management analysis. One of the steps in the process is risk analysis, wherein the collection, evaluation and study of previous cases play an important role. Risk assessment has been used in different industries and systems. Depending on the interpretation of the risk analysis, different measures and actions can be taken.
In this paper, a risk analysis will be carried out in chapter IV as part of the methodology used in this research. It will show the different hazards related to cybersecurity matters and the fact that this hazard will lead directly to damage, injury and loss in terms of safety, environmental and economic impacts.

### 3.3 Research Questions

- What kind of security measures and procedures are set up for ship owners and flag administrations against the digital reality of cyber-attacks?
- Is the virtual world a handicap for shipowners and flag administrations against cyber-attacks?
- Are the guardians of the shipowners’ and flag administrations’ systems strong enough to react when a cyber-attack is in progress and, thus, reduce the risks in terms of safety, environment, and economy?

Based on the previous question, a questionnaire was submitted to different shipping companies and flag administrations with the following questions for the purpose of gathering the necessary information to carry out a part of the analysis for this research.

**Questionnaire for shipping companies:**

1. **General:**
   1. Do you consider that cyber-attacks are an important issue that needs to be addressed by your company?
   2. How does your company classify cyber risks?
   3. Has your company been confronted with any kind of cyber-attacks in the past? Please provide details, if so.
   4. What were the main losses to your company, as a consequence of cyber-attacks?
   5. Did your company face any safety consequences caused by cyber-attacks?
6. Did your company face any environmental consequences caused by cyber-attacks?

7. Did your company face any economic consequences caused by cyber-attacks?

II. Legal: Law, Administrations, Ministry

8. Do you consider that cyber-attacks issues (on vessels, shipping companies, Administration, and in the general maritime industry) must be covered by insurance?

9. Does the insurance of your company cover cyber-attacks or technological failures?

III. Policy: Guidelines, Soft Law

10. What kind of actions or preventive measures are established in your company regarding cyber security?

11. Is there any policy or procedure regarding cyber security established in your company?

12. What type of measures are established, related to the technological system by your company in terms of recovery?

13. When was the last time that your company carried out a cyber-security assessment?

14. Do you consider it necessary to establish new regulations to address cyber security issues?

IV. Implementation: Operational Level, DPA, Crew.

15. In case of cyber-attacks, who is the person/department responsible for handling these issues?

16. Is there any response plan in place, established by your company, in case of cyber-attacks?

17. Does your company have available educational training regarding cybersecurity and cyber best practices? Please provide details, if so.
Questionnaire for Flag Administration

I. General:
1. Do you consider that cyber-attacks are an important issue that need to be addressed by your Administration?
2. How does your Administration classify cyber risks?
3. Has your Administration confronted any kind of cyber-attacks in the past? Please provide details, if so.
4. What were the main losses to your Administration as a consequence of cyber-attacks?
5. Did your Administration face any safety consequences caused by cyber-attacks?
6. Did your Administration face any environmental consequences caused by cyber-attacks?
7. Did your Administration face any economic consequences caused by cyber-attacks?

II. Legal:
8. Do you consider that cyber-attacks issues on (vessels, shipping companies, Administration, and in the general maritime industry) must be covered by insurance?
9. Does the insurance of your administration cover cyber-attacks or technological failures?

III. Policy:
10. What kind of actions or preventive measures are established in your Administration regarding cyber security?
11. Is there any policy or procedure regarding cyber security established in your Administration?
12. What type of measures have been established related to the technological system by your Administration in terms of recovery?
13. When was the last time that your Administration carried out a cyber-security assessment?

14. Do you consider that it is necessary to establish new regulation to address cyber security issues?

IV. Implementation:

15. In case of cyber-attacks, who is the person/department responsible for handling these issues?

16. Is there any response plan in place, established by your Administration, in case of cyber-attacks?

17. Does your Administration have available educational training regarding cybersecurity and cyber best practices? Please provide details, if so.

3.4 Hypothesis

The risks of cyber-attacks have made cyber-security a major concern due to the sophisticated technologies used today. Exposure and vulnerability of the different systems and the possible consequences that can affect the maritime sector are making clear the importance of addressing these issues.

Stakeholders in the maritime industry have, in recent years, developed some cyber security mitigation guidance. However, the maritime industry will need to continue working hard against cyber-attacks, pushing itself to take into consideration the guidelines provided. Nevertheless, there is a barrier in terms of making cyber-attacks public. It will be necessary that the sector consider making any internal incident of cyber-attack public since this information can serve as an example to other stakeholders, and could significantly reduce the risk and probability of cyber-attacks.

Are the shipping companies and flag administration systems strong enough to have control of their data and operations? Due to the sensitive nature of this subject matter, some difficulties have been presented in terms of the collection of data. For that reason,
a comparative analysis could not be carried out. However, as general advice for the maritime industry, it will be necessary to take into consideration the guidance mentioned above and continue to invest in actions and preventive measures to reduce the risk of cyber-attacks.

3.5 Concluding Thoughts

This chapter presents the methodology used for the research effort, which clearly shows the resources and parameter used to carry out this dissertation, with an explanation of the selected sources of collection of data and literature review. A table presents the most significant cyber-attacks cases, categorized by date, system, mean of entry, name and place of the companies involved, consequences of the attacks and small classification of the cases, with their appropriate reference. Additionally, a questioner data from a survey, which was carried out within shipping companies and maritime administration, it is presented and finalizing with a hypothesis section to conclude this chapter.
IV. ASSESSMENT OF SELECTED CYBERSECURITY CASES FROM THE LITERATURE REVIEW IN ORDER TO EXPLAIN CONSEQUENCES

4.1 Past Cyber Attack Cases

In 2015, the transportation industry was ranked in the top five industries experiencing cyber-attacks. Furthermore, a Danish shipping survey, in 2017, showed that 69 percent of shipping companies had been subjected to cyber-attacks (Figueroa, 2018). Systems used by ships, shipping companies, ports and flag states handles a significant amount of confidential and monetary information that catches the attention and interest of criminals, making these systems a target for attacks. Additionally, lack of training and human error represents a high risk for the safety of a company’s operations.

Certain cyber-attack cases in the maritime industry have been exposed to the public, including their consequences and their breakpoint related to the CIA model. The CIA model is a triad of information security used for evaluation and analysis, where C = confidentiality, the ability to ensure that data and information systems are hidden from unauthorized persons, I = integrity, the ability to assure that the data and information system are trusted, and A = availability to ensure that the data and information system are accessible and available to authorized personnel when required.

- **2011, The Islamic Republic of Iran Shipping Lines (IRISL).**

The Iranian state-owned IRISL, in August 2011, suffered significant damage to all its shipping operations data, which included loading, cargo, rate, date, place and internal company communication networks, because of cyberattacks. At the time of the attack, the shipping line was the largest in the Middle East, with a fleet of 170 vessels. The attack was concentrated in the system of IRISL. One of the consequences faced was
the data of tracking its carrier was lost, which resulted in the container movement being carried out without any company control. Some of the cargo disappeared during this period disappeared (Hutchins, 2015). The breakpoint related to the CIA model shows that, in this case, availability was disrupted. However, in due course, the data was restored and the system recovered. Nevertheless, the disruption of company operations led to cargo loss and other cargo was delivered to incorrect endpoints, resulting in a notable financial loss (Gliha, 2017). The Managing Director of IRISL, Mr. Mohammad Hussein, stated that, in relation to the considerable damage suffered due to the attack, he believes that an outside government was involved in the case (Hayes, 2016).

- **2012, Saudi Aramco, oil and gas operator.**

In 2012, the major Saudi Arabian state owned oil and gas company, Saudi Aramco, which provides 10% of the global oil suffered a cyber-attack during Ramadan month. An employee of the company opened a phishing mail with an infected link. According to Abdullah al-Saadan, vice president for corporate planning of Aramco, the primary intention behind this attack was to stop the flow of oil and gas to the international and national market (Reuter, 2012). The US investigation highlighted that the employee’s action was for sabotage purposes sponsored by another state for political motives, but no supporting evidence of this claim was presented (Perlroth, 2012). However, some files disappeared, the phone connection died, 35,000 computers shut down and three-quarters of the Aramco PC data was erased, showing that the element from the CIA model affected was availability. Nonetheless, the company, because of this attack, was unable to send or receive money transfers or contracts, nor process payments, forcing the company to stop operations and shut down its internal corporate network (Pagliery, 2015). Seventeen days after the attack, the company started to provide free oil to keep the flow of the operation with Saudi Arabia. However, it took around five months for the company, after a new security computer system was installed, to run again in normal conditions (Vella, 2016).
2012, Australia Custom and Border Protection.

Another cyber-attack in which the integrity factor of the CIA model was disrupted was the case against the Australian Custom and Border Protection cargo system in 2012. The criminal with access to the cargo system was able to use the shipper’s transport to smuggle drugs. With the ability to track cargo movements, the attacker was able to determine when the container was classified as suspicious or malicious by the police, and abandon their operation (Meyer-Larsen Nils, 2017). According to Michael Cardony, Custom and Border Protection chief, investment in an intelligent and security integrated cargo system was carried out.

2012, Danish Maritime Authority.

In April 2012, the Danish Maritime Authority was subjected to a cyber-attack. However, it was not until 2014 that the Administration discovered the attack. The attack was simply introduced by a Pdf document infected with a virus, and the virus was propagated from the Danish Maritime Authority to other government institutions before it was discovered in 2014 (Linton, 2016). Sensitive information from Danish shipping companies and merchant navy fell into the hands of hackers. In this case, the three components of the CIA model were influenced. However, according to the Danish Defense Intelligent Service report, the attack was sponsored by another state (Cyberkeel, 2014). It was difficult to assign blame without the necessary evidence, but the Danish administration had its own clues related to which state was involved in the incident. As a result of the episode, The Danish Maritime Authority shut down its whole network system for several days, and installed a new anti-virus program as a preventive measure. After the attack, an increase in security measures and the interdependency of the system was put in place (The local, 2014). This case shows that the maritime administrations are also vulnerable to cyber-attacks, highlighting that the damage they can suffer in their operational systems can directly affect important daily operations, international and national transactions and customer services as an example.
- **2013, Computerized cargo tracking and release system on Port of Antwerp.**

One very interesting incident involved the Port of Antwerp in Belgium, one of the biggest ports in Europe and in the world, which was used for drug smuggling in late 2013. The operation had been ongoing since 2011 and was discovered because a container disappeared from the port. The hacker, via a virus, infiltrated the computerised cargo tracking and release system of at least two operating companies in the port, gaining full remote control and access to the terminal system (Bell, 2013). The hacker was able to identify shipping containers where drugs had been hidden and release them to a trucker without the authorization or knowledge of the port or the shipping lines (Clark, 2017). The perpetrator then deleted information and the existence of the container from the port system. When the authorities uncovered the attack, they found 1044 kilos of cocaine, 1099 kilos of heroin, guns and more than 1.3 million Euro in a suitcase (Europol, 2013), representing only a small portion of the amount that criminals had been able to transport for two years (Bateman, 2013). In this specific case, two components, confidentiality and integrity, of the CIA model were affected. Using containers for trafficking is not new, but the fact is that criminals now have a new method for performing the acts, using technology and vulnerable systems to be more successful in their crimes.

- **2013, Oil rig Platform in USA.**

A significant incident involved an oilrig and platform in the United States of America, specifically Houston, in 2013. The incident involved malicious software downloaded unintentionally by offshore oil workers. The malware was downloaded aboard by laptops, USB drives or directly from online sources through satellites (Shauk, 2013). The files, which were infected with malware from land with pornography and music, incapacitated computers and operating systems on some rigs and platforms (Hayes, 2016). One direct effect was that one rig was paralyzed and unable to communicate with the navigation rig system, resulting in immobilization of thrusters and the navigational system. As a consequence, the Mobile Offshore Drilling Unit (MODU)
drifted from the drilling site. This incident clearly shows that the availability element of the CIA model was compromised, creating a high risk for the environment and delay in operations (Belmont, 2016).

- **2016, Vessels GPS in Korea**

In April 2016, South Korea reported that 280 vessels suffered problems with their navigational systems. The GPS signal was jammed by hackers; consequently, some of the GPS signals died and others received false information. In some cases, the GPS showed the position of vessels that were sailing on the sea as apparently being on land (Saul, 2017). When the GPS did not provide accurate information, the vessel had to return to port. The availability related to navigation equipment in respect to the CIA model was interrupted. South Korea claimed that North Korea was involved in the incidents (Graham, 2017). Nevertheless, losing a GPS signal represents a severe navigation problem, mainly if it occurs in bad weather conditions, inadequate visibility or vessel traffic areas. In these circumstances, if the GPS does not work correctly, the potential risk for a disaster with catastrophic consequences at sea is very high.

- **2017, Navigation system in a Container vessel**

The IT system of a container ship of 8,250 Twenty-foot Equivalent Unit (TEU) in the course of Cyprus to Djibouti was completely hacked in February 2017. The attack took control of the navigation system of the vessel for a period of around ten hours, making it impossible for the captain to perform navigation maneuvers (OSM, 2018). The intention of the cyber pirates, firstly, was to gain full control over the vessel navigation systems and then direct the ship to an area where they could take complete control over the ship. The availability of the CIA model was compromised and, possibly the integrity was affected as well if the vessel was completed controlled by cyber pirates. After the company provided an IT expert onboard the vessel, the crew regained control of the navigation system of the vessel. The company installed a maritime industry program to block attacks from outside that could influence the IT system. (Blake, 2017)

One clear case that shows how cyber-attacks can have a severe impact is the case of A.P. Moller-Maersk. The attack by a NotPetya Virus was directed at the port system. In this case, after massive disruptions, port operations were suspended in several port terminals controlled by Maersk division, in the United States, India, Spain, the Netherlands and other countries. No containers were received or delivered in 76 Maersk Ports, and the IT system was shut down, resulting in significant business interruption during the shutdown period. Maersk operations represent 15 per cent of all container trade worldwide (Novet, 2017).

The impact of the cyber-attack was around USD 300-400 million in lost revenue, 45,000 computers affected, and the paralysis of cargo transport through the company’s ships and ports, manifesting a significant influence on the availability component of the CIA model. This case is one of the most exciting cases presented because the attack affected ships, ports and company operations at the same time, reflecting that a compromise in one system that is interconnected represents a considerable risk for shipping operations. Additionally, the company invested in 4,000 new servers, 45,000 new PCs and 2,500 applications, all in a period of ten days (Digital Ship, 2018). However, this attack had a direct impact not only on AP Moller Maersk’s operations, but also on worldwide trade and the maritime industry in a commercial sense, giving many lessons for the industry in terms of cyber security (Guy Jon, 2018).

2017, Computer system in BW Group Singapore.

A further case involved BW Group Singapore, one of the world largest shipping companies, with a fleet that includes tankers, bulk carriers, gas carriers and offshore floating unit. The attack was severe (Mohindru, 2017). The company’s computer system was hacked, which led to its Internet and Intranet systems being temporarily suspended. During the attack, the company system was inaccessible from outside, affecting the company operations, including ports, containers, oil tanker vessels, tugboats, drilling operations, and oil and gas production, representing millions of dollars in financial loss for the company. The integrity and availability components of
the CIA model were influenced by the attacks. Although the company claimed that the attack was not related to a ransomware attempt, it shows that in the multi-billion-dollar shipping industry, cyber-security is crucial to the usual way of operation (Platts, 2017).

- **2017, Computer system of Clarkson.**

In November of 2017, one of the most famous shipbrokers, service providers and analyzers of the merchant shipping and the offshore market, Clarkson, was the victim of a cyber-incident. Clarkson’s main office claimed that the incident involved unauthorized access to the company’s computer system, reflecting that the confidentiality and integrity of the company with respect to the CIA model were compromised in all the senses. However, it did not disrupt business (Nadkarmi Namrata, 2017). The company provided an apology and tried to contact all possible clients and individuals that might have been affected by this attack; the CEO of Clarkson, Andi Case, also mentioned that “cybersecurity is at the forefront of many business agendas” (Digital Ship, 2018). As an outcome of this incident, the company immediately put in place additional security measures and took necessary actions to prevent future similar incidents, protecting clients’ data (Clarkson PLC, 2017).

- **2018, Long Beach Terminal of Cosco.**

Cosco Long Beach Terminal affiliated with Cosco Shipping was subjected to a ransomware attack in July 2018. The attack did not affect the company’s operations. However, the company decided to shut down connections with other regions, for a short period, including emails and networking phone, as a preventive measure. However, in relation to measures taken by the company the availability aspect of the CIA model was directly affected. Nevertheless, the company sent a letter to their customers to clarify the incident and make a statement highlighting that the operating system was stable after the attack and that they were working to recover from the episode (Tradewinds, 2018).
The afore-mentioned were just some cases of cyber-attacks in the shipping industry. Nevertheless, many shipping and port companies are reluctant to report incidents for fear of loss of reputation and insurance actions, emphasizing the possibility of opening a Pandora’s Box for future attacks. However, such attacks pose a risk to the integrity of vessels, ports, companies and administrations. Additionally, they represent notable economic losses for the maritime industry and possibly catastrophic consequences for human life and the environment. For that reason, jamming or disruption on any of the essential systems used in the maritime sector becomes a severe problem that can impact the maritime industry in general (Caldwell, 2010).

4.2 Risk Analysis

After the brief review of the cases presented in this chapter, the current section will present, in detail, the most significant cases of cyber-attacks in the maritime industry, with the aim of providing a real picture of the situations that are being presented by shipping companies, ports, ships and administrations through cases exposed. However, the cyber-attacks in the maritime sector are real and it is evident that the motivation of intentional direct cyber-attackers is concentrated but not limited to financial rewards. In addition, system infiltration, control and damage can be used to steal money straight from maritime companies for the purpose of carrying out weapon contraband, drugs smuggling, terrorist attacks or cyber espionage. Nevertheless, the non-intentional direct parties, such as employees, workers or crew can represent a high risk for the companies either by lack of knowledge, awareness or just pure curiosity. In such instances, the system can be affected from the inside of the company through infected email and removable media (Gliha, D, 2017).

The only element that interferes with the continuity of advances in technological systems is security and privacy. Fortunately, investment has been made in infrastructure and cybersecurity to control and prevent related problems; however, these achievements should continue and expand progressively through appropriate
investigations and studies on privacy and security, with the objective of providing new cybernetic solutions to the existing problems, instead of just focusing on new technological and interrelated systems. This approach will provide a better technological service to the maritime sector, significantly reducing the risk of cyber incidents (Farroq, Wasseem, Khairi & Mazhar, 2015).

4.3 Concluding Thoughts

In this chapter it is discussed the selected past cyber-attacks cases, giving an overview and detailed information, highlighting that more and more remote and interconnected system is used for the shipping operations, remarking that without a proper cybersecurity measure, the cyber-attacks can compromise the system and equipment affecting the respective operation. One of the important points that can bring to the table, it is the unpredictable case of Maersk, in the fact that, the attack has been performed to systems that have been used for many years in the maritime industry, demonstrating that the threats are not new. Definitively this cases marks a before and after in relation to cybersecurity issues. However, the cases presented in this chapter show that the maritime industry knows well about the contingency plan for physical disaster. Nevertheless, what about respective to the cyber world area?. One of the interesting thing for concluding, it is that compromising the vessel can compromise as well the land-based system and Vis a Vis. For that reason, the maritime industry needs to continue work hard with the all the stakeholder involved in the sector, to achieve where we want to be in a near future in term of cyber security.
V. CYBER SECURITY MITIGATION GUIDANCE AND CURRENT PRACTICES EVALUATION.

5.1 Guidelines

The shipping industry is developing day by day, with a notable worldwide role as the most efficient and cost-effective mode of transportation in international trade, involving both land and sea operations (Rosenbloom & Goldman, 1998). During the history of the maritime transportation industry, many accidents and incidents have resulted in dramatic loss of human lives, severe damage to the environment and significant monetary loss. For that reason, the industry has been subject for the development of many regulatory frameworks, and the new hot topic on cybersecurity issues is not the exception.

In this chapter, a brief summary will be presented of the Guidelines on the facilitation aspect of protecting the maritime transport network from cyber-attacks, given by the International Maritime Organization, and different guidelines on cyber security offered by different members of the maritime industry. Each of these guidelines brings to the sector an important standpoint in relation to cyber security issues, not for the technical and procedural discussion, but more for the fact that these guidelines directly influence the maritime industry to take the necessary actions against cyber threats and increase cyber awareness. At the time of this research, there are no mandatory regulations established, given that cybersecurity is a relatively new area of study (Foote, 2017).
5.1.1 International Maritime Organization

The International Maritime Organization is a United Nations (UN) specialized agency. It facilitates cooperation and information exchange among governments, wherein the mission is to promote safe, secure, environmentally sound and sustainable shipping, through effective review, development, implementation and compliance with IMO’s instruments (IMO, 2017). In the last 60 years, the organization has adopted 59 conventions and protocols and more than 1,000 codes and recommendations, representing without a doubt, that it is the only way to regulate such a complex international industry as shipping (Basaran, 2016). As a sign of this, in June 2016, IMO through the Maritime Safety Committee, released the publication of the “Interim Guidelines on Maritime Cyber Risk Management”, the main objective of which is to create awareness of the cyber awareness threat and vulnerabilities existing in the maritime sector.

The IMO guidelines are designed to provide a general overview and recommendations for cyber risk matters, focusing on risk management approach, and their incorporation by the stakeholder, which involve of digitalization, integration and automation that by different latent threat and vulnerabilities, can lead to circumstances and event compromising the safety, the secure and the operation of the shipping system.

This guideline refers to the BIMCO guidelines and the National Institute of Standards and Technology Framework (NIST), with the objective of creating a cyber-risk awareness culture at all organisational levels. The IMO guidelines include five elements that are presented in the NIST framework as well, which are identify, protect, detect, respond and recover. Identify, as the first element, shows that all systems, and personnel roles and responsibilities connected to cybersecurity should be identified. In the Protect element, the aim is to implement risk control measures, processes and contingency planning, concentrating effort on ensuring continuity of shipping operations. In the final three elements, the IMO focuses on the development and implementation process in terms of detecting, responding and recovering in case of a cyber-incident on shipping operations.
5.1.2 Maritime Industry Actors within BIMCO

The Baltic and International Maritime Council (BIMCO) and other influential maritime associations, in February 2016, released “the Guidelines on Cyber Security Onboard Ships”, designed for ship-owners and operators. The Guidelines provide assistance in assessment operations and on the implementation of actions and procedures related to preserving cybersecurity onboard vessels. This guideline is exclusively appointed to cybersecurity matters onboard vessels, with the aim of increasing cybersecurity awareness and recognizing cyber security good practice as a preventive measure against cyber-attacks in the maritime industry. According to the content of the BIMCO guideline, this includes six important cyber awareness steps: identify threats, identify vulnerabilities, assess risk exposure, develop protection and detection measures, establish contingency plans, and respond to and recover from a cybersecurity incident. Each maritime organization needs to identify the threats (internal and external), the threat possibilities and the vulnerabilities, regarding the specific risk system according to the company, trade, service or vessel operations they provide. They should understand the actual protective measures put in place, along with their capabilities and limitations.

The guideline emphasizes that the maritime industry involves many features and stakeholders, both on land and at sea, which are potentially susceptible to cyber threats. Several of the systems are related directly to safety and environmental protection. Furthermore, this guideline suggests that maritime companies and organizations should carry out an internal risk assessment to identify risk, potential threat and survey of the actual systems and procedures established, followed up by a third-party assessment. One of the most critical steps in the cyber awareness cycle, presented in the BIMCO guideline, is the development of protection and detention measures, which suggest that ship-owners and operators focus on technical defenses (ensuring the design and configuration of the onboard vessel system are resilient to cyber-attacks), and procedural defenses (covering safety and security company policy and procedures, and control of the cyber vulnerabilities). Additionally, personnel involved in ship
operations must be trained and adequately qualified. Finally, companies are encouraged to establish and maintain a contingency plan, in order to respond immediately and appropriately to cyber incidents and implement the measures developed by the company (Foote, 2017)

5.1.3 American Bureau of Shipping

The internationally recognized classification society, American Bureau of Shipping (ABS), issued a detailed series of five cyber safety guidance notes, in relation to cyber security issues. Of specific interest is “The Application Of Cybersecurity Principles To Marine And Offshore Operation”, which was published in February 2016 It has the intention to provide the members of the marine and offshore sector with the recommendations and best practices required to build and maintain cybersecurity programs. The volume contains five section. The first and second sections show a general overview of cybersecurity and present advice on cybersecurity programs. The following three sections cover the marine and offshore operations’ best practices and cybersecurity principles, where ABS promotes the implementation of the nine capabilities set for cybersecurity programs.

In September 2016, two more volumes were published, which establish standards for companies that operate offshore units and vessels on the prevention of cyber incidents that compromise the safety and security of their operations. Additionally, they refer to the verification and survey of the organizational process, as well as the carrying out audits and issue of certification, according to with the parameters provided in the guideline. Volume three concentrates on data analysis and sources, specifically data integrity concepts, which are divided into three main categories: characterising, securing and maintaining data integrity for marine and offshore operations.

Volume four and five are the Guide for Software System Verification and the Guide for Integrated Software Quality Management (ISQM), respectively. Volume four focuses on the computer control system onboard of the vessel and offshore assets, presetting diverse procedures for the verification of software and recommending that
this verification be carried out by the third party. The last volume, ISQM, is designed for managers, quality personnel and software developers, focusing on a software provider conformity program, with the intention of providing help in the improvement of the quality of software programs by the practices described in the volume.

5.1.4 Det Norske Veritas

Det Norske Veritas (DNV GL) is a maritime company that provides, in diverse fields, an advisor expertise service, with the objective of the protection of human life, environment and property. In September 2016, DNV GL addressed the issues and challenges faced by the maritime industry in relation to cyber security incidents with the publication of “Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation”. This Recommended Practice for cybersecurity risk assessment provides a clear understanding of threats, vulnerabilities, possible consequences and barriers, related to integration, digitalization and automation of systems and processes (see figure 9), for the implementation and verification of the maritime and offshore industry (DNV GL, 2016).

![Figure 9. System onboard vessel and connection to shore. Source: DNV GL](image-url)
In addition, in June 2018, a paper on cybersecurity by design, “A proposed approach applied to modern cruise ship newbuilding”, was published. This twelve-page document is intended explicitly for modern and smart cruise vessels, which require technology for operational vessel efficiency and passenger experience. This document implicates the participation of cruise operator, shipbuilding yards and marine cyber systems as stakeholders involved in the delivery process of these types of vessels (DNV GL, 2018).

5.1.5 Maritime Industry (Lloyd´S)

Cybersecurity is on the agenda of many companies involved in the maritime operational sector. As another example, Lloyd’s register, in February 2016, issued a new guidance, “Cyber-enabled Ship, Deploying information and communication technology in shipping- Lloyd’s register approach to assurance”, for a better understanding of the implications of technological systems. The guidance provides advice to different stakeholders in terms of cybersecurity matters. It contains three sections. Section two describes six specific areas of cyber risk that need to be addressed for the safety and dependability of the different interconnected systems involved in the shipping operations: system, human-system-software network and communication, data assurance and cybersecurity (Lloyd’s, 2016).

On December 2017, version 2.0 of Cyber-enabled ship, was published with the title “ShipRight procedure assignment for descriptive cyber notes for autonomous & remote access ship”, Lloyd’s register guidance document. This document is designed for vessels classed by Lloyd’s Register, with the purpose of assessing systems installed onboard that are manipulated by crew but can be monitored and controlled remotely or autonomously as well. For that reason, the risk-based approach needs to consider the variation that this system brings to the table, and which is discussed in this version (Lloyd’s, 2017).
5.2 Present Risk Mitigation Analysis
Questionnaire for shipping companies and Maritime Administrations.

A questionnaire related to cybersecurity issues was sent to different maritime administrations and shipping companies, with the aim of obtaining current information on the actions and preventive measures adopted today. As mentioned in the limitation section, many shipping companies and maritime administrations refused to participate in this survey because they consider that the subject matter is a sensitive topic to discuss. However, regarding the answers received, it can be concluded that:

1. The vast majority of those surveyed agreed that security and cybersecurity is a very serious topic, which can not only affect the safety of shipping operations, but also the safety of the employees and the personnel involved in each activity.

2. Most of the companies and maritime administrations claim that they take into consideration the necessary measures to address this critical issue, mentioning that the IT system protection, cybersecurity awareness, contingency measures and training of the personnel are considered in the internal procedures of the companies and administrations.

3. The responses show that each company and maritime administration has different ways of classifying cyber risk. This is due to the fact that each company and administration has its portfolio of the services, and in the relation to that, the classification has different variables.

4. The survey also revealed that some of the companies and the maritime administration have experienced small cyber incidents, such as network trouble, application error, phishing attempts, malicious emails and other minor incidents.

5. The responses show that no major incident has been recorded, and no major losses, as a consequence of cyber-attacks have been faced.
6. No safety, environmental or economic effects as a result of cyber-attack, has been confronted. The survey highlights that the risk of cyber-attack is very high and could have severe consequences in the maritime industry.

7. The study demonstrated the concern of the shipping companies and maritime administration in terms of insurance, considering that the insurance companies need to take into consideration cyber-attacks and their consequences to provide adequate coverage.

8. The survey also revealed that cyber-attacks have many types of possible outcomes, which is one of the primary challenges. However, the fast evolution and influence of the industry means that more insurance companies carry out studies in this regard, and include cyber-attacks in their insurance services.

9. The shipping companies and maritime administration surveyed implement cyber threat identification, security manuals and technical training as established preventive measures.

10. It is considered by the respondents that a new regulation is required, taking into consideration that technological systems and equipment are continually evolving, so new revisions and new measures need to be considered to maintain up-to-date regulations related to cybersecurity.

11. It is noted that each shipping company and the maritime administration have dedicated personnel and security officers responsible for handling cybersecurity issues. However, they highlight that security is everyone’s responsibility and the most optimal way to address these issues is with education and training.

12. The survey revealed that a response plan has been put in place by the shipping companies and maritime administration surveyed.

13. The majority of those surveyed mention that training courses are necessary and many of them already put in practice these courses for shore-based and seagoing personnel, to keep up-to-date, understand the risks and vulnerabilities, and reduce the
possibilities of cyber-attacks. Nevertheless, training is not enough. It is necessary to take into consideration exercises and practices to ensure that the personnel is aware of the issues and that the course will not just be a box ticking exercise.

5.3 Barriers for Cyber Security Implementation
In this section, the most significant barriers are identified and presented below, in terms of implementation of cyber security measures.

5.3.1 Cost or Lack of Resources
The cost of cyber security measures represents a substantial financial loss for the company. However, this section highlights that a cyber-attack will cost more in the end than if preventive measures were taken in the first place. For many companies, the financial limitation and the lack of resources is a big issue. The budget that is designated for security matters is limited, which is ironic because the security of the system that controls all the operations of the company should be a priority. However, it is understandable that for many small companies investing in cybersecurity will represent a great economic challenge, but it is necessary to prioritize spending on cyber security measures. The main considerations should be investment in cybersecurity training and awareness, cybersecurity controls, antivirus, operational system measures and an insurance that covers cybernetic attacks (Schweigert, 2017). Nevertheless, according to Healthcare Information and Management Systems Society (HIMSS) Cyber security survey 2018, allocation of cyber security resources was a business priority for companies in the last year.
5.3.2 Ignorance and Ignoring

Firstly, ignorance relates to people that do not know about the matter. They lack knowledge of the security measures most applicable to their systems, and the different packages available. They do not know if they are investing in something really safe or if they are being scammed. It is for that reason that it is necessary that the companies have a qualified person that can ensure the cybersecurity conditions of the company and feel sure that the investments they are making will be worth it. However, there is another aspect to discuss and it is ignoring. This is mostly related to the Ostrich Algorithm, which is a strategy of putting your head in the sand and ignoring potential problems. This is basically the action of many companies that know that there is an issue requiring prompt decision, but prefer to ignore it and act like there is nothing happening. This attitude represents a very high risk for them, their customers, their partners and the stakeholders involved in the service that the company provides (Schweigert, 2017).

5.3.3 Control and Monitoring

In order to apply effective control and monitoring in terms of cyber security, it is essential, firstly, to determine cyber security priorities, to move ahead for compliance, and to define the best practices that need to be implemented. When this is set up, it is necessary to maintain a control and monitoring of the system and operations that are related with interconnectivity and network (Whitterker, 2016). Additionally, it is essential to have appropriate cybersecurity personnel, which according to the HIMSS survey 2018, represent the most significant barriers for remediating and mitigating cybersecurity incidents. For that reason, the training and qualification of personnel (see chapter VI Recommendations) has become a key supporting element to consider, not only for control and monitoring aspects, but as a safeguard for the company and personal security (BIMCO, 2016).
5.4 Concluding Thoughts

As it is presented in the previous chapter, the cyber-attacks can result in loss of communication, information, data, navigation, propulsion, time, cargo, casualties, business disruption and losses as an example. However, the guidelines discussed focus in the vessel, mobile offshore units, marine and offshore operation and vessel manager perspective. Nevertheless, it is essential that the shipping company, follow the guideline mentioned in term of understand the threats, risks, vulnerability and possible consequence that each system and equipment related to vessel operation can have, highlighting that for 2021 will be included in the International Safety Management Code (ISM Code), which will be a regulatory framework for cyber risk assessment, and for 2022 audit and Port State control Inspection will be carried out to verify their compliance.

On the other hand, port, shipping companies and maritime administration need to take the necessary preventive measure and action to reduce the probabilities of being cyber-attacks, emphasizing that any system and equipment connected to internet is 100% secure, there is always the possibility to be cyberattacked, but the preventive measures as a real risk assessment, company security policy, education and training, contingency plan, etc., can reduce significantly the probabilities of being cyber attacked or reducing the consequences.

The barriers analysed in this chapter demonstrate that the companies can present some difficulties in term of implementation, for that reason the barrier discussed in this chapter need to be taking into consideration for the shipping industry. Therefore, the question that came to my mind is, if the shipping companies did not take the appropriated cybersecurity measures, for how long the companies, port, vessel and maritime administration can survive, after a sever cyber-attack.
VI. DISCUSSION AND CONCLUSION

6.1 Discussion of Findings

According to all the previous chapters, the maritime industry is clearly vulnerable to cyber-attacks. Today, shipping companies, vessels, ports and maritime administrations have various modern electronic systems, facilitating profit and conduct of their daily operations. However, this technology, if it is not used adequately and along with the proper security measures, could have serious repercussions. There is a lack of understanding within the maritime industry of what cyber-attacks really mean and the consequences followings these incidents.

It is necessary to understand that the risks that the maritime industry is facing in terms of cyber security are real. For that reason, it is necessary that the management team engages in the cyber security issues explained in the recommendation section because a cyber-attack is an organizational problem, not just related to the IT department. These issues can directly affect the whole organizational structure and enterprise operation.

It is also important to carry out an evaluation of the best practices and an assessment of the systems, equipment and products, that will be used by shipping companies, ports, vessels, maritime administrations before investing in a new technological system or equipment. This will help to verify whether or not this modern technology represents a risk to the company, society, environment and individuals. Nevertheless, the future of cyber-attacks in the maritime industry is difficult to predict; the time to act is now.
6.2 Conclusions

In the new digital era of the maritime industry, where information and communication technology play an imperative role, systems will be more interconnected, remote controlled, network dependent and possibly autonomous. The market has been transformed from the traditional concepts used during previous centuries. The new technologically advanced systems that are present in the modern shipping industry facilitate efficient operation, but at the same time represent specific vulnerabilities for the different systems, which can result in catastrophic scenarios.

In conclusion, there is no doubt that today the maritime sector is safer, secure, environmentally friendly and energy efficient, compared with previous decades, and it is evident that it is not lacking in international regulatory frameworks, representing an absolute advantage as a transportation mode (IMO, 2017). However, the constant evolution of the shipping industry, the manifestation of new technology and other contemporary challenges make it eminent to elaborate a long-term plan. This need is reflected in the United Nations’ and IMO’s proactive agenda, with an influential position to achieve the sustainable development goals (UNEP, 2013).

The cyber security issue is strongly affecting the maritime industry. Since the beginning, it has been necessary to have the collaboration and participation of all the stakeholders involved in the shipping industry, but the issue is that, due to the sensitive nature of the subject matter, it is difficult to collect more data to carry out a more in depth investigation. Further investigation needs to be carried out to continue showing the importance of the cyber-attacks affecting the maritime industry and the future difficulties that will be presented in the sector. Nevertheless, the participation of the shipping industry is necessary to contribute to creating better operational conditions, implementing and enforcing national regulations and contributing to the stability and prosperity of maritime trade. This will help to ensure that the maritime industry continues to play a vital role in the world economy, and will ensure better future conditions for the new generations. (IMO, 2017). For that reason, it is important that regulatory organisations, shipping companies, vessels, ports and facilities keep
working on the development of cybersecurity protection measures to safeguard intellectual property, vessels, ports and facilities from cyber threats.

6.3 Limitations

The limitation presented during the development of this research was in terms of the collection of data and feedback from the questionnaire. It has been observed that information, procedures, and implementation regarding cyber-attacks are confidential to many shipping companies, ship owners and flag administrations. Additionally, there is an inclination in the sector to keep cyber incidents secret, with the fear of being exposed to more cyber-attacks, resulting in loss of reputation and negative business consequences.

6.4 Recommendations

The maritime industry in the last years has taken significant steps concerning developing guidelines and recommendations to address cybersecurity issues. However, it is evident that with the continued grow and demand for technological systems and equipment used in daily shipping operations, there is a necessity for the industry and government to continually develop and implement strong measures and take the necessary actions to focus on cybersecurity. The following recommendation aims to present an alternative to promote and increase policy, procedures, training and culture in terms of cybersecurity in the maritime sector (See figure 10).

![Figure 10. Recommendations. Source: Author](image-url)
6.4.1 Promote Cybersecurity Policy and Procedures

The promotion and implementation of the cybersecurity policy and procedures is essential for the maritime sector against cyber-attacks. It is indispensable that the policy and procedures developed and implemented for the maritime companies include safety and security strategy, scope, goals, risk assessment, responsibilities and roles, operational procedures, training and awareness, security and safety requirements, operational security, incident management and a recovery plan.

Cybersecurity insurance needs to be considered as a contingency plan taken by shipping companies, ports, maritime facilities, and other business infrastructures involved in maritime operations. It is necessary that the maritime business review policies to verify which aspects of cybersecurity incidents and losses are covered by insurance, including user training and education, network security, malware protection, security configuration, monitoring process and incident management.

6.4.2 Promote a Cybersecurity Risk Aware Culture

According to a relevant cyberkeel report, the human element involved in maritime operations is the most vulnerable one in terms of cybersecurity. For that reason, it is necessary to develop a training strategy on cyber security awareness for employees. Shipping companies, governments, port facilities, ship-owners and operators, as the main stakeholders involved in shipping operations, need to develop a culture of cyber risk awareness at all operational and technical levels.

For the promotion of a cybersecurity risk aware culture, it is indispensable that the management level of companies take the necessary actions against cyberattacks, promoting education and training of all personnel that has access to a sensitive system, raising awareness of cyber threats and vulnerabilities. As a result of these actions, a total organizational cybersecurity culture will be created.
6.4.3 Promote Sharing Information among Maritime Industry

In order to manage cyber security issues, information sharing is a crucial factor to take into consideration. In general, shipping companies, vessels, ports and maritime administrations face many common threats daily. However, facilitation of information sharing is vital to help other companies in the maritime industry to better understand the current panorama and take proactive actions immediately. As is presented in the limitations section of this dissertation, one of the difficulties presented during the development of this research is that many shipping companies, ports and maritime administrations prefer to keep cyber incidents confidential. This is for fear of repeated cyber-attacks, and/or for prevention of reputational effects.

Another important factor that should be considered is cyber threats reporting, as is the case of the United State Coast Guard, which, in 2016, issued a “reporting cyber-attacks and suspicious activities” policy, where the vessels and marine facilities are required to report to NRC any of the abovementioned scenarios. The reporting of cyber incidents can be beneficial when a study and analysis is carried out with the aim of provided clear recommendations that can be shared throughout the sector to help avoid future incidents.

6.4.4 Promote Tailored Training And Awareness.

The normal functioning of the shipping industry is based on human interaction, qualification and knowledge. As a result, maritime education and training play an essential role in the development of the sector. Firstly, education is a primary part of the seafarer’s life. Having well-educated and trained seafarers can reduce many risks, such as those related to shipping, cargo, and navigational operations that are presented in the seafarers’ daily life.

Talking about the cybersecurity issues, vulnerability, risks and consequences previously presented, The International Convention on Standards of Training, Certification and Watchkeeping (STCW) should be considered. Currently, there is almost nothing relating to cybersecurity education and training for seafarers and
especially for deck officers. To address the issues related to cybersecurity onboard vessels, it is necessary that IMO take into consideration the development of training courses for seafarers and deck officers, specifically in cybersecurity topics to educate seafarers in the correct use of technology onboard vessels and introduce the risks that the vessel system and equipment may have in terms of disruption.

Notwithstanding, shipping operations are just a small part of the interconnected maritime industry. Shipping companies, ports and maritime administrations need to take the necessary measures in relation to training of personnel that work directly with sensitive systems and information that can be jeopardized by cyber-attacks. An internal training plan on cybersecurity, which can include the risk of using e-mail, internet, personal devices, removable media, and passwords, as well as awareness of data practices, installing and maintaining software, suspicious activities, quick response and contingency planning, and impacts and consequences needs to be developed with the aim of promoting awareness on the use of technological systems.
VII. REFERENCES


Clark, J & Donal, K. (2017). Shutting the stable door after the cyber horse has bolted. Retrieved from: https://www.porttechnology.org/technical_papers/shutting_the_stable_door_after_the_cyber_horse_has_bolted


Novet, J. (2017, August). Shipping company Maersk says June cyberattack could cost it up to $300 million. CNBC. Retrieved from:


APPENDIX SECTION

Appendix 1: Definitions

1. Botnets: According to Techtarget a bonnets can be defined as a collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware (Techtarget, 2018).
2. Bugs: Techopedia define bugs as an error, fault or flaw in any computer program or a hardware system (Techopedia, 2018).

3. Cybercrime: is the use of computers or related systems to steal or compromise confidential information for criminal purposes, most often for financial gain (Katzan, 2012).

4. Cybercriminal: It is define for Tredmicro as, individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit (Trendmicro, 2018).

5. Cyberespionage: is the use of computers or related systems to collect intelligence or enable certain operations, whether in cyberspace or the real world (Katzan, 2012).

6. Cyberspace: According to Oxford dictionaries, cyberspace is the notional environment in which communication over computer networks occurs (Oxford dictionaries, 2018).

7. Cyberterrorism: is the use of computers or related systems to create fear or panic in a society and may not result in physical destruction by cyber agitation (Katzan, 2012).

8. Cyberwar: consists of military operations conducted within cyberspace to deny an adversary, whether a state or non-state actor, the effective use of information systems and weapons, or systems controlled by information technology, in order to achieve a political end (Katzan, 2012).

9. Hacktivist: The Oxford dictionaries define hacktivist as a person who gains unauthorized access to computer files or networks in order to further social or political ends (Oxford dictionaries, 2018).

10. Insider attacks: According to Techopedia, an insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access (Techopedia, 2018).

11. Jamming: is the (usually deliberate) transmission of radio signals that disrupt communications by decreasing the signal-to-noise ratio, resulting in the loss of the
link’s reliability, increased energy consumption, extended packet delay, and disruption of the end-to-end routes (Guirguis, 2012).

12. Phishing: refers to the process of deceiving recipients into sharing sensitive information with a third-party (BIMCO, 2016).

13. Ransomware: Ransomware is defined by techopedia as a type of malware program that infects, locks or takes control of a system and demands ransom to undo it. Ransomware attacks and infects a computer with the intention of extorting money from its owner (Techopedia, 2018).

14. Spoofing: Techopedia define spoofing in general, as a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security (Techopedia, 2018).

15. Spyware: According technopedia Spyware is infiltration software that secretly monitors unsuspecting users. It can enable a hacker to obtain sensitive information, such as passwords, from the user’s computer. Spyware exploits user and application vulnerabilities and is often attached to free online software downloads or to links that are clicked by users (Techopedia, 2018).

Appendix 2: Electronic magazine survey
Which of the following electronic maritime magazines do you know?

- Lloyd’s List
- Digital Ship
- Tradewinds
- Fair Play
- Otra...
- Agregar una opción

Which of the following electronic maritime magazines do you know?
53 respuestas

- 7 (13.2 %)
- 12 (22.6 %)
- 19 (35.8 %)
- 50 (94.3 %)

MSc in Maritime Affair, World Maritime University, Sweden
How often do you read any of this magazines?

- Once a week
- Once a month
- Once a Year
- Otra...
- Agregar una opción

How often do you read any of this magazines?

52 respuestas

- Once a week: 18 (34.6%)
- Once a month: 22 (42.3%)
- Once a Year: 4 (7.7%)
- Once in 2 months: 1 (1.9%)
- Every day: 1 (1.9%)
- Once in 6 months: 1 (1.9%)
- Four times year: 1 (1.9%)
- It depends with the contents: 1 (1.9%)
- Not regular: 1 (1.9%)
- Sometimes not regular reading: 1 (1.9%)
- 5 times a week: 1 (1.9%)
<table>
<thead>
<tr>
<th>Time</th>
<th>Electronic Maritime Magazines</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018/09/07 3:26:14 p.m. GMT+2</td>
<td>Lloyd List; Fair Play, Lloyd’s List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 3:51:18 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Lloyd’s List</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 3:57:36 p.m. GMT+2</td>
<td>Lloyd’s List; Digital Ship, Fair Play</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 4:00:07 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Fair Play, Lloyd’s List</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 4:04:08 p.m. GMT+2</td>
<td>Lloyd’s List; Digital Ship, Fair Play, Lloyd’s List</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 4:08:19 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Fair Play</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 4:09:36 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Digital Ship</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 4:11:05 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Fair Play</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 4:14:37 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Nautilus UK</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 4:18:22 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Gcaptain, Clipping News (Maasmond Maritime)</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 4:19:39 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Fair Play, Lloyd’s List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 4:21:44 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Fair Play</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 4:24:40 p.m. GMT+2</td>
<td>Lloyd’s List; Digital Ship, Lloyd’s List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 4:26:07 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 4:28:58 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 4:29:58 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 4:33:15 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Fair Play, Lloyd’s List</td>
<td>Once in 2 months</td>
</tr>
<tr>
<td>2018/09/07 4:37:27 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Lloyd’s List</td>
<td>Once a Year</td>
</tr>
<tr>
<td>2018/09/07 4:40:07 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 4:44:23 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 4:45:24 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Lloyd’s List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 4:46:03 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Lloyd’s List</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 4:46:24 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List</td>
<td>Every day</td>
</tr>
<tr>
<td>2018/09/07 4:46:51 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List, BIMCO, DNV GL</td>
<td>Once in 6 months</td>
</tr>
<tr>
<td>2018/09/07 4:48:42 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List, Maritime Executive</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 4:54:58 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List, Lloyd’s List</td>
<td>Four times year</td>
</tr>
<tr>
<td>2018/09/07 5:01:56 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 5:03:30 p.m. GMT+2</td>
<td>Lloyd’s List; Bimco, Lloyd’s List</td>
<td>Once a Year</td>
</tr>
<tr>
<td>2018/09/07 5:05:13 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 5:07:18 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Fair Play</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 5:17:18 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 5:21:28 p.m. GMT+2</td>
<td>Lloyd’s List; Digital Ship, Lloyd’s List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 5:24:30 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 5:25:20 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Lloyd’s List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 5:27:45 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 5:28:20 p.m. GMT+2</td>
<td>Lloyd’s List; Tradewinds, Lloyd’s List</td>
<td>It depends with the contents</td>
</tr>
<tr>
<td>2018/09/07 5:29:08 p.m. GMT+2</td>
<td>Lloyd’s List; Fair Play, Lloyd’s List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 5:31:18 p.m. GMT+2</td>
<td>Lloyd’s List; full avant news, Lloyd’s List</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 5:36:33 p.m. GMT+2</td>
<td>World’s Maritime News</td>
<td>Once a week</td>
</tr>
<tr>
<td>Date and Time</td>
<td>Sources</td>
<td>Frequency</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>2018/09/07 5:38:21 p.m. GMT+2</td>
<td>Lloyd's List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 5:42:36 p.m. GMT+2</td>
<td>Lloyd's List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 6:16:01 p.m. GMT+2</td>
<td>Lloyd's List; Digital Ship; Tradewinds; Fair Play</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/07 6:33:04 p.m. GMT+2</td>
<td>Lloyd's List</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 6:33:07 p.m. GMT+2</td>
<td>Lloyd's List; Fair Play</td>
<td>Once a Year</td>
</tr>
<tr>
<td>2018/09/07 8:30:26 p.m. GMT+2</td>
<td>Lloyd's List; Fair Play</td>
<td>Sometimes not regular reading</td>
</tr>
<tr>
<td>2018/09/07 8:35:05 p.m. GMT+2</td>
<td>Lloyd's List; Fair Play</td>
<td>5 times a week</td>
</tr>
<tr>
<td>2018/09/07 9:56:57 p.m. GMT+2</td>
<td>Lloyd's List; Digital Ship; Navigator</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/07 11:50:55 p.m. GMT+2</td>
<td>Lloyd's List; Fair Play</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/08 1:54:00 p.m. GMT+2</td>
<td>Lloyd's List</td>
<td>Once a month</td>
</tr>
<tr>
<td>2018/09/10 8:48:31 p.m. GMT+2</td>
<td>Lloyd's List; Tradewinds; Fair Play</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/12 1:07:38 a.m. GMT+2</td>
<td>Lloyd's List; Fair Play</td>
<td>Once a week</td>
</tr>
<tr>
<td>2018/09/12 8:24:37 p.m. GMT+2</td>
<td>Lloyd's List</td>
<td>Once a month</td>
</tr>
</tbody>
</table>
Appendix 3: Electronic Magazine Collection of Data

Digital Ship Magazines:

Edition 124 August 2017 page 35
Edition 124 August 2017 page 3
Edition 125 October 2017 page 3
Edition 126 November 2017 page 33
Edition 128 February 2018 page 12
Edition 129 April 2018 page 14
Edition 130 June 2018 page 2018
MSc in Maritime Affairs, World Maritime University, Sweden
Fairplay Magazines:


Lloyd’s List Magazines:

7 June 2017
28 June 2017
7 July 2017
14 July 2017
16 August 2017
16 October 2017
7 November 2017
29 November 2017
21 March 2018
20 July 2018
25 July 2018
27 July 2018
30 July 2018
31 July 2018
Search Results

Search

cyber

Showing 1 - 10 of 313 results for "cyber"

14 Sep 2018 NEWS
LLOYD'S LIST
The Lloyd's List Podcast: From Brexit to IUMI
By Lloyd's List
Lloyd's List The Shipping Podcast

Search

cybersecurity

Showing 1 - 10 of 74 results for cybersecurity

14 Sep 2018 NEWS
LLOYD'S LIST
British ports told to brace for autonomous ships
By Anastassios Adamopoulos
A new report warns vessel autonomy will mean changes in port infrastructure as well as more highly skilled personnel
United Kingdom Technology and Innovation Regulation

19 Jul 2018 INTERVIEWS
LLOYD'S LIST
Shipping failing to deal with threat of cyber crime
Tradewinds Magazines:

06 July 2017
27 July 2017
28 July 2017
16 October 2017
29 November 2017
09 February 2018
25 July 2018
30 July 2018
31 July 2018
08 March 2018