11-4-2018

# Cyber-security and marine insurance

Davit Dadiani

**WORLD MARITIME UNIVERSITY**

**Malmö, Sweden**

# CYBER-SECURITY AND MARINE INSURANCE

**By**

**DAVIT DADIANI**
**Georgia**

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 LAW AND POLICY)**

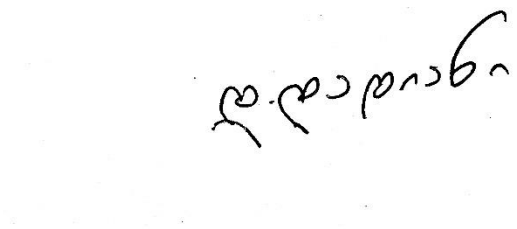
2018

# 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):



(Date): 18 September, 2018

Supervised by: Henning Jessen, Ph.D. (Dr. iur)

World Maritime University

Supervisor's affiliation: Maritime Law and Policy

**ACKNOWLEDGEMENT**

First of all, I would like to thank TK Foundation for the opportunity to study at the World Maritime University. The experience I gained at the University is truly amazing.

I would like to express my sincere gratitude to my professor and supervisor Dr. Henning Jessen. His dedication, keen interest in my research, recommendations, meticulous scrutiny and scientific approach has played an enormous part in my research.

I am grateful to all the professors and lecturers that have taught me and all the staff employed at the World Maritime University, especially Maritime Law and Policy professors: Max Mejia, Aref Fakhry, María Carolina Romero Lares, George Theocharidis and Laura Carballo Piñeiro.

I am extremely thankful to my wife Mariam, my family and friends for supporting me throughout my studies.

I am thankful to my professors from Georgia Maia Bitadze and Eka Siradze for helping me to pursue my education at the World Maritime University.

And of course, I would like to thank country of Sweden and city of Malmö for the wonderful days I have spent there.

## ABSTRACT

Title of Dissertation: **Cyber-Security and Marine Insurance**

Degree: **Master of Science**

The dissertation is a study of current approaches of marine insurance regarding cyber-security. The study reviews scope of coverage of cyber-risks by the marine insurance industry.

A brief look is taken at the definitions of cyber-attacks from marine insurance point of view. All the relevant international instruments and documents are being considered and analyzed in order to determine current international legal frameworks regulating cyber-security.

The study shows how Marine Insurance Act 1906 and cyber-risks are related. Comparative analysis between the traditional marine risks and the cyber-risks was done. Analysis articulates that the cyber-risks are already the marine perils endangering the shipping industry.

All of the major the P&I Clubs' rules are examined in the study. The problem of identification of cyber-risks by the P&I Clubs' is articulated in the paper.

In concluding remark, the study gives thoughts how can marine insurance can deal with the cyber-attacks.



Key words: cyber-security, cyber-attack, marine insurance.

# Table of Contents

## List of Abbreviations

| | |
|---|---|
| AIS | Automatic Identification System |
| BIMCO | Baltic and International Maritime Council |
| CLIA | Cruise Lines International Association |
| EU | European Union |
| GPS | Global Positioning System |
| ICS | International Chamber of Shippin |
| IMO | International Maritime Organization |
| INTERCARGO | International Association of Dry Cargo Shipowners |
| INTERTANKO | International Association of Independent Tanker Owners |
| IT | Information Technology |
| IUMI | International Union of Marine Insurance |
| PIN | Personal identification number |
| P&I | Protection & Indemnity |
| OCIMF | Oil Companies International Marine Forum |
| TEU | Twenty-foot Equivalent Unit |
| USB | Universal Serial Bus |

# Chapter 1. Introduction

## *1.1. Background*

In June of 2017, the shipping company A.P. Moller-Maersk (the world's largest containership operator) experienced a cyber-attack. The cyber-attack affected the company's container shipping, port and tugboat operations, oil and gas production, drilling services, and oil tankers (Maersk says the global IT breakdown was caused by the cyber-attack, 2017). The cyber-attack costed A.P. Moller-Maersk between $250m and $300m and around one month to recover (Porter, 2017). Singapore-based BW Group (one of the world's leading maritime groups in the tanker, gas and offshore segments) also suffered from the cyber-attack in July of 2017. However, the company did not specify the financial effects of the attack (BW Group Computers Hit by a Cyber-Attack in July, 2017). The Maersk and BW Group cases are just two examples of how vulnerable the international maritime trade can be to cyber-attacks.

## *1.2. Problem Statement*

The modern shipping industry is becoming more and more integrated into technological advancements and the cyber-world, like many other different fields of international economies. Complex cargo systems are using digital utilities, cranes are using satellite-based GPS systems, maritime navigation systems are connected to information technology systems, the Automatic Identification System (AIS) is used by larger vessels (Cyber Risks and Insurance in the Marine Industry, 2016) and

Inmarsat is using GPS (Global Position System). These technological systems are responsible for handling the vast amount of money, ships, cargo and other properties owned by international maritime companies.

However, cyber-attacks are the new threat to today's world: hackings, security breaches and stolen data. All of these risks are becoming frequent. On the other hand, marine insurance can be a "tool" which should play a crucial role in helping the international maritime trade to recover from cyber-attacks. In the context of the maritime industry, the risks are associated with two general objectives: a) cyber-attack on vessels; b) a cyber-attack on the corporate offices of maritime companies, which are equipped with digital devices and computers to run their businesses.

Nowadays cyber-attacks are not enough acknowledged as a specific and particular threat by the marine insurance community, which creates both legal and financial vacuums to avoid future risks. Like many other major risks, which are covered by marine insurance (natural disasters like cyclones, earthquakes, lightning, theft, violence, and piracy), cyber-attacks have grave effects on the maritime industry.

Threats are changing from cyber-attacks. Companies in all business sectors are under highly sophisticated and complex attacks, which are targeted to damage property and operations by seeking to take control of industrial operating systems (The Risk of Cyber-Attack to the Maritime Sector. 2014) or maybe to steal certain data in order to demand a ransom. This has happened with the well-known shipbroker Clarksons PLC (Clarksons Warns of Possible Data Leak After Cyber Attack, 2017). The significance of the issue was addressed at Global Liner Shipping Conference held on 6 September 2017, where one of the speakers, Toby Stephens (from the global law firm "Holman Fenwick Willan") mentioned that the shipping industry must be prepared or the attack will affect the bottom line of industry since the industry has a blind spot (Shipping firms have no excuse for being vulnerable to cyber-attacks, 2017).

Insurers acknowledge the dangers of cyber-attacks, however, understanding the problem is the main issue. Further, appraising the price of the exposure is the main barrier that stops the marine insurance industry to tackle the problem (maritime

companies are not declaring information to the public if they have experienced cyber-attacks, due to the fear of losing clients, the decline in stocks and are afraid to scare the shareholders). The above-mentioned problem leads insurers to exclude cyber-attack losses from policies, incorporating into the policies, the "paramount clause" - Cyber Attack Exclusion Clause (CL 380) 10/11/2003 (The Risk Of Cyber-attack To The Maritime Sector, 2014). This clause excludes any loss, damage, or liability caused, either directly or indirectly, by the use of a computer and its associated systems and software. Another problematic issue, which the marine insurance industry faces, is the term "cyber". "Cyber" is the very broad term, which may include many different features, characteristics and details. For insurers, it is very hard to formulate one particular mechanism to resolve the problem. Also, it is very important to realize that each cyber-attack is one single incident, which threatens, for example, a single ship (The Guidelines On Cyber Security Onboard Ships, 2017).

The international community and organizations have been reluctant to address the issue with certain legislation. So far, the issue has not been addressed in a proper manner like other threats. However, the maritime industry is not the only one which is starting to feel the "pain" from hackers. Atlanta, capital city of state of Georgia (U.S.A.), was held by the hackers for ransom. Police officers used to fill reports on paper, residents could not pay bills and the courts were frozen (McArdle, 2018).

With the evolution of both international maritime trade and modern technologies, the more interconnected these two sectors become. Therefore, in the future cyber-security will be the main threat to the international maritime trade sector. The Marine insurance industry must be prepared with specific knowledge how to handle cyber-risks. More needs to be done to educate insurance companies and support them by providing specific scientific research materials.

Cyber-security becomes a more and more important issue. For the sustainable and safe development of economy, modern society needs to pay more attention to the cyber-security awareness raising.

### *1.3 Aims of the Research*

The aims of the research are to:

1. discuss approaches in the marine insurance industry related to cyber-security risks and liabilities, in order to identify if cyber-security is covered by the insurance companies;
2. discuss the scope of coverage practice adopted by the insurance companies;
3. discuss the future solutions for the marine insurance industry to cover the cyber-security risks and liabilities.

### *1.4 Objectives of the Research*

The main objectives of the research are:

1. to analyze the scope of cyber-security coverage through marine insurance;
2. identify the most problematic issues which are creating the obstacles for marine insurance companies to include cyber-security in their insurance policies;
3. to analyze legislation and judicial decisions of the United Kingdom related to marine insurance;
4. to discuss contractual drafting practices and methods of approach of the marine insurance companies which are covering cyber-security related losses;
5. to review certain cases of cyber-attacks on the shipping companies and identify the main aspects of cyber-attack threats;
6. to compare losses caused by cyber-attacks and losses which are covered by marine insurance;
7. to highlight the significance of cyber-security risks/liabilities;

8. to discuss the role of the International Maritime Organization (IMO) in supporting the marine insurance industry with guidelines and technical cooperation in a fight with the growing threat of cyber-attacks.

### *1.5. Methodology and Ethical Issues*

Due to the complexity of the research topic, different research methods were used together. The research has been conducted mainly through qualitative methods. The research uses the fundamental approach to gather all the information it needs to find a solution. During the research two types of methods were used in general: descriptive research and analytical research. For the practical research the following methods were used:

1. Interviews – from representatives of the P&I Clubs (member associations of International Group of Protection & Indemnity Clubs) - the research uses both the semi-structured interview and the in-depth interview styles depending on the content of the interview and the respondent's significance in the topic - interviews have been conducted through online interviews (email) - data analysis of the interview was used transcribing and coding - the end report used for verification. The research used a moderate participatory approach for participant observation - data collection and data analysis was conducted through field notes and research diary;

2. Content Analysis - conceptual analysis - - the research reviewed both scientific and legislative sources of the research topic - data collection: articles, books, journals, publications, web-sites, P&I Clubs' circulars and rule books, and other reliable sources were used during the research in order to identify the key issues of marine insurance and cyber-security. The sources mentioned above was explored through different online search engines (web-portals) and with printed material from World Maritime University's library shelves. For the case study research, the exploratory case study was used in order to understand the issues of marine insurance and cyber-security.

During the research, marine insurance judicial decisions were discussed for the purpose of the objectives of research.

### *1.6. Expected Results*

The research highlights the importance of cyber-security issues and threats to the maritime sector. A growing number of cyber-attacks on shipping companies must be addressed since their participation in the world economy and international trade is enormous. Marine insurance is a tool that can be used to answer to the losses caused by cyber-attacks. The research provides an outlook of the current situation in marine insurance coverage related to cyber-attacks (identification and clarification of issues associated with complexity covering cyber-attack risks and liabilities through marine insurance) and will propose the general key points which will help the marine insurance industry to address cyber-security as a part of the risk and liability of their policies (fundamental discussion and analysis of cyber-security threats).

The research is expected to be used as guideline thoughts for future researchers of marine insurance and cyber-security. It will be used for the clarification risks and liabilities of cyber-security, that fall in marine insurance coverage.

### *1.7. Potential Limitations*

1. The number of participants to adequately draw conclusions;
2. The constantly changing nature of cyber-attacks;
3. The confidentiality of marine insurance companies related to the cyber-attack announcements which they experienced.
4. The non-linear approaches of the marine insurance industry;
5. The potential lack of specific scientific literature.

## Chapter 2. Cyber-Attacks as a New Challenge to Marine Insurance

### *2.1. Definitions of Cyber-Attack*

From the marine insurance perspective, it is very important to legally define the term "cyber-attack". Nowadays, there are many different types of contracts and clauses which define the terms for the purpose of the contractual obligations. Distinct terms are used in industries across the world to define a "cyber-attack" generally, but for the marine insurance objectives the general term should be at least connected to (a) a shipping company; (b) a ship owning company; (c) a charterer; (d) port management company or other port handling organization. Each cyber-attack on shipping industry is one single incident, one single activity, although it could last some certain period of time (The Guidelines On Cyber Security Onboard Ships, 2017).

The research concentrates specifically on cyber-attacks connected to the shipping and maritime industries, although the definition of "cyber-attack" can be defined in many different ways depending which sector is a target of attack.

The most important actors of the marine insurance, the P&I Clubs, publish different documents and guidelines regarding the cyber-security which defines "cyber-attack". The definitions drafted in these documents are very important for analyzing how the marine insurance industry itself sees cyber-attack and cyber-risk. Alongside the P&I Clubs it is very important to analyze also how cyber-attack is defined by IMO and other international organizations:

The important definitions of cyber-attacks and cyber-risks:

- According to UK P&I Club Q&A document (2018): "Cyber risks can be defined as the risk of loss or damage or disruption from failure of electronic systems and technological networks" (p. 1).
- BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI produced "The Guidelines On Cyber Security Onboard Ships" (The Guidelines On Cyber Security Onboard Ships, 2017) states that " Cyber-attack is any type of offensive manoeuvre 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." (p. 44).
- IMO Interim Guidelines On Maritime Cyber Risk Management published on 1st June 2016 (MSC.1/Circ.1526) "…maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised." (p.1).
- In its P&I Loss Prevention Bulletin published in May of 2018 (Vol. 42) Japan P&I Club provides a definition of cyber-risk: "Cyber-risk" is a potential risk to lead to operation failure of the IT systems, which will cause financial loss, disruption or damage to the reputation of an organization. Cyber-risk includes external factors (such as computer virus, Trojans, or attack over network, etc.) and internal factors (malfunction, miss-operation, or system bug, etc.)." (p. 17).
- North P&I Club specifies that cyber-risk may be the failure of an onboard GPS receiver due to a fault with the equipment, extending right through to the catastrophic scenarios of vessel systems being attacked and the vessel being disabled, run aground or taken over by malicious third parties (Cyber Risks in Shipping, 2017).

Analyzing the above-mentioned definitions is the next step to summarize what are the distinct characteristics of "cyber-attack" in the maritime world. First, *an intentional act by third party*. Second, purpose of the cyber-attack is *to (a) damage or destroy the vessel or cargo on the vessel; (b) damage the shipping company/ship-owner company's reputation; (c) access and compromise the information the third party holds to use it in malicious way.* Third, it is done through *offensive action against*

*vessel's electronic and/or computer systems, technological networks, IT and OT systems or any other connectivity or electronic process or device connected to the vessel.*

### *2.2 An Overview of the Effects of the International Instruments on Cyber Security*

According to Ole Vidar Nilsen from DNV.GL: "We do not want to present cyber security as the hooded criminal hacker, but as part of safety and security on vessels. For example, every ship conducts fire and lifeboat drills, but do the crew prepare for a cyber-attack? We want to influence good behavior and a good attitude by managing this, for many new risks." (Cyber Security Awareness, 2018). The preparation of crews aboard regarding the cyber-security should be more proactive and even mandatory if the shipowners want their vessels to be cyber-secure.

With the increased threat coming from the cyber-attacks on the whole shipping industry, the international maritime community is under pressure to deliver the policy documents which will eventually influence future international treaties to regulate cyber-security. IMO as global standard-setting authority for the safety, security and environmental performance of international shipping should play a major role in setting the regulatory framework for cyber-security. With the increased risk of cyber-attacks IMO has published the Guidelines On Maritime Cyber Risk Management (IMO Guidelines On Maritime Cyber Risk Management, 2017).

The law regulating the marine insurance is private in nature. The parties of the marine insurance sign legally binding agreements, they enter a contractual relation and are bound by the obligations written in the agreement. Currently, there is no international convention regulating cyber-security in the maritime sector, and that means there is no mandatory insurance covering cyber-attacks. However, there are several international conventions that specifically address marine insurance. For example, International Convention on Civil Liability for Oil Pollution Damage (1992), International Convention on Civil Liability for Bunker Oil Pollution Damage (2001)

and Nairobi International Convention on the Removal of Wrecks (2007) all requiring from shipowners to have insurance. The above-mentioned examples demonstrate how public international law elements could be involved to direct contribution from the marine insurance industry. With growing threat coming from cyber-attacks, the requirement for international instrument governing cyber-security becomes highly relevant.

There are several important instruments to be noted that are discussed below regarding the cyber-security:

### 2.2.1. International Ship and Port Facility Security (ISPS) Code

The International Ship and Ports Facility Security (ISPS) Code (SOLAS XI-2 and the ISPS Code, 2018) - establishes regulatory cooperative standards for the detection of security threats, precautionary measures against security incidents, security- related information exchange standards, security assessment methodology.

Part B of the ISPS Code articulates that both The Port Facility Security Assessment (PFSA) and Ship Security Assessment (SSA) must address radio and telecommunication systems, including computer systems and networks.

### 2.2.2. International Safety Management (ISM) Code

The Maritime Safety Committee, on 16th of June 2017, adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems (Resolution MSC.428(98), 2017). According to the Resolution, an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code.

The Resolution encourages the administrations of the flag states to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

For the shipping companies operating a vessel complying the ISM Code is very important. From the marine insurance perspective, it will be interesting how the marine insurance will react in the future on ships which are not complying with cyber risk management. Can the shipping company insure their fleet which are poorly cyber-risk-managed? Will the insurance companies let shipping companies insure ships which are not properly cyber-managed? Should due diligence principle apply on seaworthiness of such ships?

The ISM Code has the potential to develop as an instrumental standard of vessel cyber-security. Complying with cyber risk management will fall under the principle of loss minimisation (What are the Five Principles of Marine Insurance?, 2018).

### 2.2.3. IMO Guidelines On Maritime Cyber Risk Management

IMO issued the Guidelines on Maritime Cyber Risk Management (IMO Guidelines on Maritime Cyber Risk Management, 2017) on 5th of July 2017. The Guidelines introduces the general elements and principles that every shipping company can include in their practices. The Guidelines introduce several functional elements for shipping companies in dealing with cyber risk: identification, protection, detection, response and recovery.

The mentioned vulnerabilities in the Guidelines may be caused by malicious actions like hacking or introduction of malware. This wording is very important to identify internationally the risks coming from cyber-attacks. So far, it is the first instance from IMO to articulate such risks. This means the maritime industry as whole, not only the marine insurance industry, should consider more thoughtfully regarding

cyber-risks. IMO as a standard setting authority in safe and secure shipping is aware that risks are not only coming from hacking or introduction of malware, but also from the unintended consequences of benign actions. The maritime industry is less protected when outdated software is used on board a vessel.

It is still unknown whether IMO will contribute more in the future in cyber issues and risks. However, it is a big step forward for the maritime industry in raising the awareness in cyber-security issues. It is the first fundamental instrument in the hands of IMO in regulating the cyber-risks and could be the basis for more complex regulations in the future.

### 2.2.4. ISO/IEC 27001 Standard On Information Technology

The International Organization for Standardization (ISO) has also addressed the issue and published a series of standards regarding cyber-security. ISO/IEC 27001 (ISO/IEC 27000 Family - Information Security Management Systems, 2018) is a series of standards and they are made to help organizations manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties. ISO/IEC 27001 are providing requirements for an information security management system (ISMS). ISMS is a systematic approach to managing sensitive company information so that it remains secure.

These standards are very helpful and important for shipping companies and also for vessels to adopt in their practice. It is a basic safety measure for vessels to avoid any kind of mismanagement and help the safe-keeping of their information.

### 2.2.5. The Guidelines On Cyber Security Onboard Ships

Industry leaders BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI have released the joint "The Guidelines on Cyber Security Onboard Ships" (The Guidelines on Cyber Security Onboard Ships, 2017). The Guidelines are a comprehensive document which addresses the cyber-security issues on board. The Guidelines are important, since the document was drafted by the industry representatives and not IMO, therefore giving it insight of the industry's response to the risks.

The most important part from the BIMCO Guidelines is the threat identification section. According to the guidelines, the perpetrators of cyber-attacks are: activists (including disgruntled employees), criminals, opportunists, states/state sponsored organizations/terrorists. These named perpetrators have one common aim – a deliberate attack. The motivations are different for each actor, but the most important from the marine insurance perspective are: reputational damage, disruption of operations, financial and commercial gain.

The Guidelines also name the objectives of the cyber-attack: destruction of data, publication of sensitive data, media attention, denial of access to the service or system targeted, selling stolen data, ransoming stolen data, ransoming system operability, arranging fraudulent transportation of cargo, gathering intelligence for more sophisticated crime, exact cargo location, off vessel transportation and handling plans. This information could be extremely useful for the marine insurance business to appraise the risks. The Guidelines take a comprehensive approach to encompass all the damages and losses that could be caused by a cyber-attack.

### 2.2.6. Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA)

The SUA Convention (Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988) is another international convention which in certain ways relates to cyber-security issues, but it is specifically designed to fight terrorism across the world.

The possibility that cyber-attacks could be used for terrorist purposes is high (McNicholas, 2016). Therefore, SUA Convention and terrorist cyber-attacks could be linked. Article 3(1) provides the scopes of offense by a person:

*"1. Any person commits an offence if that person unlawfully and intentionally:*
*(a) seizes or exercises control over a ship by force or threat thereof or any other form of intimidation; or*
*(b) performs an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship; or*
*(c) destroys a ship or causes damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship; or*
*(d) places or causes to be placed on a ship, by any means whatsoever, a device or substance which is likely to destroy that ship, or cause damage to that ship or its cargo which endangers or is likely to endanger the safe navigation of that ship; or*
*(e) destroys or seriously damages maritime navigational facilities or seriously interferes with their operation, if any such act is likely to endanger the safe navigation of a ship; or*
*(f) communicates information which he knows to be false, thereby endangering the safe navigation of a ship; or*
*(g) injures or kills any person, in connection with the commission or the attempted commission of any of the offences set forth in subparagraphs (a) to (f).".*

Analyzing the wording of subparagraphs and definitions, terrorist cyber-attack falls under the scope of the SUA Convention. The characteristics of the cyber-attack

has the same features as an unlawful act against the safety of maritime navigation: a) cyber-attack could lead to seizing control over a vessel by threat (for example if the hackers threat to destroy navigational communications of a vessel); b) cyber-attack can destroy cargo by switching off the refrigerators of a vessel; c) USB flash drive with malicious virus could be used to sabotage a vessel; d) cyber-attack could interfere with navigational operations through GPS; e) the hackers could easily send a false information about navigation of a vessel. Ransomware – has very similar features to the offences listed in SUA Convention: it is a threat to steal data or give the data to the public; it is unlawful and it is intentional.

Even the cyber threats were not common when the SUA Conventions was adopted, but its broader and flexible terms can clearly be linked to cyber-attacks.

### *2.3 Cyber-Security and Maritime Security*

Current threats to maritime security arising from the cyber domain are also very important to discuss. In 2013, with the help from two hackers, a Dutch transnational criminal organization conducted a series of criminal activities. They smuggled several containers loaded with cocaine into the port of Antwerp (McNicholas, 2016).

The authorities started to investigate when, the containers were disappearing after arriving at the importers sites. After investigating the case the authorities found that the hackers had sent malicious emails to the port workers. The port workers then opened and downloaded the email contents. After that their computers became inflicted with the malicious programme and was an easy target for the next cyber-attacks. Thus, the hackers accessed all the information connected to the Gate Dispatch systems, Terminal Container Yard Management systems and vessel arrival and manifest systems. They changed the cargo release data and were enable to pick-up containers before a real buyer came. However, in the system it showed that the containers never left the terminal.

Cases like that are already happening. It is not only the criminal organizations, but also the state actors who are involved. Major players like China, Russia and Iran on the international scene are already using cyber-capabilities to threaten maritime security (McNicholas, 2016).

Terrorism has not been so threatening to maritime security until now, however, the Somali pirates and terror groups like al-Shabaab already have infiltrated the online maritime tools to hijack vessels. However, the risk will rise when these groups actively recruit hackers to achieve their missions (McNicholas, 2016).

Responding to the risks, many states have started to prepare themselves. In 2014 the UK drafted "The UK National Strategy for Maritime Security" (National Strategy for Maritime Security, 2014). The document mentions "Attack on UK maritime infrastructure or shipping, including cyber attack" one of the maritime security risks from 2014-15 (Bueger, 2015). Therefore, one of the major maritime countries in the world is already adapting its national security documents regarding maritime cyber security.

In recent years the gas networks are starting to integrate more digital services (Myrvang, 2018) into their operations. Data gathering, analysis and visualization to maintain, repair and operate gas networks are all operations that could be done using digital systems. Digitalizing the gas networks has its own vulnerabilities. Cyber-attacks on digitalized gas networks could lead to lost production; raised health, safety and environmental risk; costly damages claims; breach of insurance conditions; negative reputational impacts; and loss of license to operate. It is not only the natural gas networks, but also oil networks.

Natural gas and oil networks in the seas have strategic economic security implications for many countries. Their economy depends on the secure and safe gas or oil imports and exports. Not to mention how many different jurisdictions the networks cross. Powerful cyber-attacks could sabotage international maritime security. Industry leaders in quality assurance, risk management and classification activities DNV.GL have published guidelines how to apply International Electrotechnical Commission's IEC 62443 standard covering security for industrial

automation and control systems (DNVGL-RP-G108 Cyber Security in the Oil and Gas Industry Based on IEC 62443, 2018).

The above-mentioned trends will play major roles in the future of maritime security. There are new stakeholders in international maritime security and they are called – hackers. Nowadays it is extremely hard to identify who they are, who stands behind them and their aims vary with each case. It could be sabotaging large offshore oil drilling platforms and causing major oil catastrophes or provoking big countries maritime powers; for example, China's Ministry of State Security hacked into the US Naval Undersea Warfare Center's contractor and stole six hundred fourteen gigabytes of data. The information contained top-secret submarine communications data and information on a secretive project known as Sea Dragon (Morris, 2018).

So, it is not only marine insurance to be concerned with the situation, but the international community should address the growing threat and to find common ground among the states.

## Chapter 3. Cyber-Security and Legal Aspects of Marine Insurance

### *3.1. Marine Insurance Act 1906 and the Impact of the Reform*

A discussion about the cyber-risks of marine insurance must include the analysis of the applicable UK legislation, particularly the Marine Insurance Act 1906 (Marine Insurance Act 1906, 2018) which laid the fundamentals for marine insurance rules, not only in the UK, but also around the world.

The UK legislation was instrumental in forming not only the marine insurance law, but influencing the whole maritime law in general. Therefore, analyzing the Marine Insurance Act 1906 is important for this research.

The biggest challenge when analyzing the Marine Insurance Act 1906 is whether the cyber-risks and cyber-security challenges could comply with the principles and rules of the Marine Insurance Act 1906 if the marine insurance will incorporate cyber-attacks as a marine risk. Does the one century old legal act regulate the challenges arising just few years ago? The cyber issues are not like anything else humankind has ever experienced, also considering from the legal point of view.

With increased pressure coming from the cyber-security threat, the problem is to either bring new amendments into the Marine Insurance Act 1906 or to interpret existing provisions of the law as a regulating framework for marine insurance and cyber-attacks. Innovative amendments could fundamentally change how marine insurance will deal with cyber-attacks in the future.

The UK legislation is a common law system and without the judicial decisions of courts and similar tribunals regulating cyber-security is very difficult. With the speed the cyber-attacks are developing and changing, the marine insurance industry will sooner or later witness litigations in the UK courts.

However, Marine Insurance Act 1906 will still face real challenge if it can regulate furthermore cyber-risks. A completely new act from the Parliament of the UK could be more helpful for the marine insurance industry.

### *3.2 Cyber-Attack as a Marine Risk*

Section 1 of the Act defines that marine insurance is contracted in order to "indemnify… against…the losses incident to marine adventure". For comparative research, it is important to analyze several case scenarios in order to identify a cyber-attack on a ship as a cause of incident to marine adventure. For example, the vessel that was taking a voyage from port A to port B was attacked by a malicious computer virus (released on purpose by the hackers targeted on the vessel or without any specific target released in order to attack any potential victim) through its communications network. The virus blocked or altered navigational devices and other electronic

mechanisms on board and was grounded or lost part of its cargo. Elements of section 1 could be then applied to the case. The fact that the vessel was en route from one port to another and suffered from a "cyber-attack" implies "losses to marine adventure". The nature of the action to be considered has two elements, "marine adventure" and "losses", where both elements could be applied to the above mentioned case scenario (Arnould, Gilman, & Merkin, 2008).

The insurable interest is defined in section 5 of the Act:

*(1) Subject to the provisions of this Act, every person has an insurable interest who is interested in a marine adventure.*

*(2) In particular, a person is interested in a marine adventure where he stands in any legal or equitable relation to the adventure or to any insurable property at risk therein, in consequence of which he may benefit by the safety or due arrival of insurable property, or may be prejudiced by its loss, or by damage thereto, or by the detention thereof, or may incur liability in respect thereof.*

Section 5(2) does not provide an all-inclusive definition, however it defines legal and equitable "relation" (Bennett, 2006). This was drafted to also cover the case law before the Act came into force. According to Susan Hodges, persons mentioned in section 5(1) can be divided in three main categories: (a) owner of insurable property like shipowner and cargo owner; (b) persons who have lent money on the security of ship or cargo and (c) insurer itself (Hodges, 1996).

It is unclear whether damage to software and computer systems would be considered "physical damage to tangible property" — as required by a standard marine insurance policy (Cyber Risks And Insurance In The Marine Industry, 2016).

However, it is safe to assume that broad definition of insurable interest could be in favor of the future interpretation of assured's insurable interest in vessel's or cargo's safe and due arrival and insuring from cyber-attacks.

Insurable interest covers different types of insurances. For property insurance like hull/machinery and cargo, assured's interest will be proprietary and contractual. Insurance of freight, hire and profits the assured's interest is a freight. Insurance of freight has two approaches. Traditional approach states that when a vessel starts a

freight-earning journey only then rises inchoate right which supports insurable interest (Bennett, 2006). However, there is also a case law contradicting the traditional approach, which according to the case law insurable interest starts when a vessel is fully ready to begin a freight earning journey. For liability insurance, the insurable interest could be linked to the reason of casualty during the journey of a vessel (Bennett, 2006).

Covering cyber-attacks could not be as simple as traditional marine risks are. It will depend what will be the consequences of the cyber-attack. First, cyber-attack on a vessel as mentioned before could be linked to property. At the minimum, a vessel's electronic devices that are fundamentally important to navigate and maneuver, might be damaged. The assured would have insurable interest in property in this case. Or the cyber-attack on a vessel's navigational systems can lead to a collision or grounding of a ship. The refrigerators of a vessel could be switched off by the hackers and the cargo can deteriorate. These examples articulate that the assured's insurable interest of cyber-risk insurance could be proprietary.

The complexity of covering cyber-risks is that the assured's insurable interest can also be freight, for example if a vessel is attacked by the hackers and the severity of cyber-attack leads it be stuck in the sea for long period of time. This leads to loss of profit and freight.

The liability and P&I insurance of the assured's insurable interest could be casualty during the journey of a vessel. The risk of vessel encountering third party liability when it is under cyber-attack is high.

### *3.3 Applicable Principles of Marine Insurance*

Analyses of cyber-security implications on the marine insurance should not be discussed without mentioning the core principles applicable to them. This research

concentrates on the following core principles: due diligence, duty of fair presentation, warranties and principle of *Causa Proxima*.

### 3.3.1. Duty of Utmost Good Faith

One of the most important principles of the Marine Insurance Act 1906 is "utmost good faith" articulated in section 17: "A contract of marine insurance is a contract based upon the utmost good faith". The law of marine insurance imposes a duty of "utmost good faith," or *uberrimae fidei*.

It is worth noting that the principle before the amendments postulates that the parties to contracts must not only avoid fraud and misrepresentation, but they are required to disclose voluntarily "every material circumstance" (Schoenbaum, 1998). The principle of utmost good faith is vital for an insurer because the assured has much more information before signing a contract and the insurer is dependent only on the information given by the assured. The principle defends the rights of the insurer into the imbalance between him and the assured (Bennett, 2006). Even with such vast information given to the insurance companies today, the assured are directly dealing with the information (Bennett, 2006) and having a more advantageous position compared to the insurer. This issue could be pivotal in a cyber-risk insurance. First, does the assured knows well every important thing to disclose to the insurer before filling in the insurance policy? IHS Fairplay survey showed that only 30 percent of those responding to the survey had no appointed information security manager or department (Rider, 2018), then how could those 30 provide all the needed information to the insurance companies?

Regarding cyber-security, the assured should provide the information to insurance companies related to every electronic system, electronic devices, operating systems, communication, GPS or navigational facilities. The information should relate to the electronic devices performance and level of their working conditions. In this area the particular nature of the information could be challenging for the insurer.

Taking into consideration the difficulty of dealing with special electronic devices on board the insurance companies should adjust their working principles to IT knowledge.

According to Lord Mansfield in the English case of Carter v Boehm: *"... good faith forbids either party, by concealing what he privately knows, to draw the other into a bargain from his ignorance of that fact, and from his believing to the contrary"* (Hemsworth, 2018). The information to be provided to the insurer must be reliable even without checking it, otherwise the insurer can avoid signing the insurance agreement.

In the case of cyber-security providing the information beforehand, this is complicated. The main problem in this area is that there would be situations when even the shipowner or the captain of a vessel, are not fully aware about conditions of their hardware and software systems installed on board. European Union Agency for Network and Information (ENISA) conducted a study regarding the cyber security challenges in the maritime sector, which states that maritime cyber security awareness is currently low, to non-existent (Analysis of Cyber Security Aspects in The Maritime Sector, 2011).

### 3.3.2. Due diligence

Full disclosure of relevant information for the insurance is a key principle of the marine insurance (Schoenbaum, 1998). Bearing in mind that shipping companies, shipowners, marine insurance companies and the P&I Clubs like every commercial organization are sensitive about their confidential information due diligence is an important issue.

To exercise due diligence by the parties before signing a legally binding contract will play an important role when insuring cyber-risks. Due diligence conducted on electronic devices of a vessel would subsequently include existing cyber

guidelines and standards adopted by the shipping company or required by the insurance company. The companies should be able to disclose all electronic data held on the ship which contains vital information for a ship's normal functioning. It may be privacy policies, computer systems controls, seafarer's privacy information, cargo carried by the ship, communication systems used by a particular ship.

If IMO's and other "cyber hygiene" instrument guidelines are not fully and properly implemented by the shipowner the insurer could refuse to cover losses or damages caused by cyber-attacks because *"failure to implement the procedures and risk controls"* (Andrews & White, 2017).

Another key issue connected to due diligence is the discovery or occurrence of cyber-attack. Detection of such an incident, and discovery of their scope, is a vital fact for insurers. Another point is when cyber-attack never occurs, however, there are reports of such an incident. It could lead to reputational damage for the assured company.

There are very fundamental steps taken in past years regarding the due diligence for example, ISM and ISPS Codes could be a fundamental tool for exercising due diligence regarding the cyber-security on the ships. From 2021, the ISM Code will introduce cyber risk management guidelines (Resolution MSC.428(98), 2017). For the shipowners, the ISM Code's cyber risk management guidelines will be part of the requirements in order to exercise their rights of due diligence. Oil Companies International Marine Forum's (OCIMF) Ship Inspection Report Program (SIRE) requires from shipowners to ensure that cyber risks are properly addressed (Textor, 2017). OSIMF released Tanker Management and Self Assessment (TMSA), which recommends that an internal cyber audit program must be conducted, owners should retain independent cyber specialist support, and they must update vessel ISM System/SMS and ISPS ship security plans to address cyber security risks.

### 3.3.3. Warranties

Warranties have an important role in marine insurance (Soyer, 2001). Marine Insurance Act 1906 covers warranties in sections 33-41; according to the Marine Insurance Act 1906 section 33(1):

*"A warranty, in the following sections relating to warranties, means a promissory warranty, that is to say, a warranty by which the assured undertakes that some particular thing shall or shall not be done, or that some condition shall be fulfilled, or whereby he affirms or denies the existence of a particular state of facts"* (Marine Insurance Act, 1906). If the warranty is breached the insurer is not liable any more from the moment of the breach, however, the insurer is still liable for any insured losses before the breach has happened (Marine Insurance, 2015).

Warranties are divided into two categories: Expressed warranties and implied warranties. Express warranties expressed in the policy are part of the contract, while implied warranties are not drafted into the contract but they are understood by the parties (Soyer, 2001). For cyber-security, implied warranties are especially relevant, bearing into mind the warranty of seaworthiness.

Seaworthiness of the ship is defined in the Marine Insurance Act 1906, section 39(4): "*where a ship is deemed to be seaworthy when she is reasonably fit in all respects to encounter the ordinary perils of the seas of the adventure insured*." The definition is broad and general, and it is not limited to the particular technical features of a vessel. The seaworthiness of the ship was defined also in case of Gibson v. Small (Soyer, 2001). According to the definition of seaworthiness the ship is connected to the state of the ship and the perils it could encounter, and it is mutually important that a prudent owner uninsured would continue his voyage.

Therefore, from a cyber-security perspective, when the ships are all "armored" with different types of electronic devices which could be easily infiltrated through the cyber-attack the duty of providing the seaworthy ship (Soyer, 2001) could be the applied duty of providing a cyber-secure ship and when talking about equipment and

stowage the first questions should be: is the equipment secured from cyber-attacks? Are radars, charts, refrigerators and engine seaworthy and can resist cyber-attacks? Concluding the warranty of the seaworthiness of the ship and cyber-security is a far reaching topic, considering in mind that seaworthiness is a rather detailed description of the ship. Therefore, section 39(4) could be applied to the seaworthiness of the ship related to the cyber-security.

### 3.3.4. Causa Proxima

There is an opinion among the insurance experts that cyber-attack must be "successful" to be considered as a risk (Moss, 2018). However, there is another issue to be considered also. Can "unsuccessful" or "partially successful" cyber-attacks should be considered as a marine risk. What about the attempt to cyber-attack a vessel? According to section 55(1) of the Marine Insurance Act 1906, *"Subject to the provisions of this Act, and unless the policy otherwise provides, the insurer is liable for any loss proximately caused by a peril insured against, but, subject as aforesaid, he is not liable for any loss which is not proximately caused by a peril insured against."* The section defines the proximate cause (*causa proxima*). But the Marine Insurance Act 1906 does not provide any information about method for determination of the proximate cause of a loss (Gürses, 2017).

For the cyber-attacks to determine the proximate cause could be very difficult. For example, the cyber-attack is untraceable and it does not leave any kind of evidence that there was such an incident, but the crew onboard witnessed the cyber-attack. This kind of scenarios could be frequent in the future. Concurrent Causes is another issue that marine insurance can face when covering the cyber-risks. For example, if the hackers caused severe disruption in the navigational systems of the vessel, but meanwhile the master of the vessel had not updated the navigational systems software in due time which could have easily avoided the cyber-attack.

## Chapter 4. The Risks and Liability Issues of Cyber-Attacks

Cyber-attack risks are often associated with demands for ransom payments, and losses such as interruption to business, reputational damage and potential liabilities to other parties. Cyber-Attack on a ship could lead to a physical risk for the vessel. Modern vessels are connected to many types of different communications to navigate and operate. The communications systems orchestrate a vessel's navigational routes. Technologies like the Automated Identification System (AIS), Electronic Chart Display & Information System (ECDIS), Global Navigation Satellite System (GNSS) and E-Navigation Systems (E-Nav) are omnipresent among the vessels. Main and auxiliary propulsion systems are operated by computer technologies (Roche, 2016). All these issues create dangerous access for the hackers or other perpetrators to carry out attack.

Dividing cyber-risks by its original aims into two sub-categories – (a) deliberate attack on a vessel and (b) non-deliberate attack on a vessel - the risk of a vessels physical damage could be the same if key systems are lost at crucial times.

There are two differences between the existing usual marine risk and the cyber-risk. The most obvious difference between the usual marine risk and the cyber-risk is that the cyber-risk can only be addressed by experienced maritime professionals' with full support of specialized IT consultants (Roche, 2016).

The second difference is cyber-risks further consequences. A cyber-attack could lead to collision, personal injury, property damage, pollution or even to a shipwreck (Cyber Risks and P&I Insurance, 2018). Therefore, from the marine insurance perspective the cyber-risks could expand from property categories like hull

and machinery loss/damage and cargo loss/damage, to income loss of hire and to liability protection and indemnity (P&I).

### *4.1. Damages and Losses of Cyber Attacks*

Since 2013, over 9 billion records have been lost or stolen from all around the world generally. A single large scale cyber-attack can trigger $53 billion in economic losses (Extreme Cyber-Attack Could Cost as Much as Superstorm Sandy, 2017). According to some analysts, 2021 cybercrime will cost the economy $6 trillion (Desjardins, 2017). Allianz, the leading insurance and financial service company, published Allianz Risk Barometer 2018. According to the report business interruption and cyber incidents will interlink as the major threat for companies through 2018 and beyond, according to the insight of 1,911 risk experts from 80 countries (Allianz Risk Barometer 2018, 2018). The cyber-risk was named the second most important business risk after the business interruption risk according to the Allianz Risk Barometer 2018.

In July 2018, Cosco suffered a ransomware cyber-attack; even some months later the company was still affected from the attack. The attack caused the breakdown of company's networks and systems in the US, services such as slot booking and emails being affected throughout the world (Shen, 2018). In a statement the company acknowledged the existence of "ransomware". Kidnap & Ransom Insurance (K&R insurance) is one of the risk insurance products existing on the marine insurance market. The difference between the demanding ransom for paying hostages aboard the vessel and demanding ransom for not releasing the sensitive and confidential information.

Damages and losses affected by cyber-attacks are confidential information and the shipping companies are reluctant to publish it. The issue of confidentiality has a negative side, although there are new initiatives. CSO Alliance has started a new project called, Maritime Cyber Alliance, anonymous online reporting service (Baker,

2018). With Maritime Cyber Alliance, everyone from shipping company or from a vessel, can report a cyber-incident. For example, one anonymous person published a story about a cyber-attack that lasted 150 days on a shipping company that resulted in a $500 000 payment interception. The problem may be that publishing information about significant losses may lead to the reputation damage of the company or it will also affect shareholder's decisions about further investing in the company.

When analyzing how cyber-attacks affect marine insurance it can be concluded that there are two general consequences. From the perspective of the marine insurance cyber-attacks, losses and damages can be divided into (a) property damage and loss (hull, machinery, cargo) and (b) reputation damage.

### *4.2 Stakeholders/Parties of Cyber-Incidents*

Marine insurance will face another challenge in determining the cause of a cyber-incident. The identification of persons involved in a cyber-incident is important and interesting from marine insurance perspective.

Further, besides the traditional parties of the marine insurance insurer and assured, there are several actors who could play a major role in a cyber-incident:

- The seafarer, captain of a vessel or any member of a crew– (a) negligence of a seafarer injecting USB flash drive into the computer on board, which is infected with virus and thus causing the incident or (b) opening virus carrying email in the computer on board (Cyber Security – Understanding Risk Simply, 2018).
- Pirates – trying to hijack the vessel and navigate it into a trap or asking for a ransom;
- States or state sponsored/affiliated persons – trying to disrupt another states vessel;
- Terrorists trying to carry out terrorist acts involving a vessel;

- Hackers trying to get information about a vessels movements and sensitive information and in order to sell it.

All the above-mentioned persons could be initiators of cyber-incidents on board of the ship, which could result in a catastrophic scenario for the ship. The goals and aims of each person who caused the particular cyber-incident is extremely important to clarify the different risks associated with IT security. Parties involved in the cyber-attack should be very important for the marine insurance perspective and marine insurance companies should draft their contracts and policies dealing with those incidents.

### *4.3. Liability Problems*

Confidentiality plays a huge role in shipping industry (Baker, 2018). Many shipping companies are privately held companies which have lesser obligations for reporting (e.g. annual reports) and lesser obligations for transparency, compared to publicly traded companies. Therefore, the private companies are keen to keep all kinds of information only for themselves. This means that evaluating the cyber risks and assessing the problem is difficult.

There are some new challenges the companies face about confidentiality and data protection. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Regulation (EU) 2016/679 Of The European Parliament and of The Council, 2018) enters into force in 2018 and it will have certain effect on publicity of the data and information held by the shipping companies (Adamopoulos, 2018). Regulation (EU) 2016/679 will have an influence on the disclosure of cyber-attacks and data breaches. The provisions of the regulation requires companies that have suffered a data breach to report it to the relevant authorities and the people whose data was affected within 72 hours.

As a result, it is expected that the Regulation (EU) 2016/679 will push the shipping businesses in Europe to report cyber-incidents. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union (Directive (EU) 2016/1148 of the European Parliament and of The Council, 2016) is another significant instrument in the hands of EU for regulating cyber-security. The provisions of the Directive set out standards for Member States to identify essential service operators, define national strategy on security networks and information systems, appoint national competent authorities and single point of contact, create notification system and set computer security incident response teams. The EU, since its foundation always was pioneer in implementing innovative and strict legal frameworks for regulating strategic industries, and this Directive is an example of that. Both the above-mentioned Regulation (EU) 2016/679 and Directive (EU) 2016/1148 will influence defining and identifying the cyber-risks and therefore marine insurance will play a significant role to ensure these risks.

However, there are many other jurisdictions where no legislation regarding the cyber-security is adopted. It is also worth mentioning that he European Union Agency for Network and Information Security (ENISA), the European Defence Agency (EDA), Europol and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) signed a Memorandum of Understanding (MoU) to establish a cooperation framework among their organisations (Four EU Cybersecurity Organisations Enhance Cooperation, 2018). The cooperation will encompass several areas: exchange of information, education and training, cyber exercises, technical cooperation and strategic and administrative matters. The cooperation will facilitate a more active role in determining the occurrence of cyber-incidents, therefore it will help both the public and private sectors.

The problem of liability of marine insurance would be uncertainty of a cyber-incident's cause. That means the marine insurance companies and P&I Clubs have to prepare for new liability scenarios, as responsibility shifts from human to machine, from the ship crew or ship management to ships computers and electronic devices.

Cyber-attacks are not only coming from hackers', technical failure or innocent employee action, which is often to blame. Moreover, liability can lead to the manufacturer or its suppliers, with assignment and coverage of liability becoming more challenging (Allianz Risk Barometer 2018: Future Risks, 2018).

Cyber-insurance provided by marine insurance would also face another challenge: If a vessel suffers a data breach, for example, it will need instant access to specialist lawyers, IT experts and crisis management consultants to help mitigate the impact of an incident as it develops. This means that risks covered by the insurer should encompass expenses associated with mitigating the immediate damages and losses caused by cyber-attack. However, the marine insurance will face another challenge in assisting mitigation processes when a vessel is at the sea far away from the port of call with no IT expert on the board (Blake, 2017), which means that cyber-attack will be more severe for the vessel and it can last longer without reaching the nearest port.

The problem of liability will also be if experts, official public authorities or any other IT specialist organization cannot detect the cause of the cyber-attack.

Stealing data from a vessel or shipping company that is valuable for vessels normal transportation to avoid collision or any other peril may be analogized with loss of goods, loss of cargo carried by a vessel. According to this theory, cargo insurance should be activated between insurer and assured. Whereas a cyber-attack damages or destroys a vessel, hull and machinery insurance should be addressed.

The characteristics of a cyber-risk is another noteworthy thing to discuss. Cyber-attack maybe caused by criminals for example but not limited to pirates. On the other hand, cyber-risk can be caused by non-criminal activities, for example, seafarer injects the USB flash drive carrying malicious computer virus into a vessel's electronic system which, in the end causes electronic systems on the board have severe outages (Eling & Hendrik Wirfs, 2016).

The doctrine of *uberrimae fidei*, plays an important part in marine insurance. The doctrine requires the insured "*to disclose to the insurer all known circumstances that materially affect the insurer's risk, the default of which … renders the insurance*

*contract voidable by the insurer*." It is very hard to determine at what level the shipping companies are ready to expose their information to the insurance company when procuring the cybersecurity insurance (Cyber Risks And Insurance In The Marine Industry, 2016).

# Chapter 5. Current Approaches and Practices of the Marine Insurance Industry

## *5.1 A Case Study Example: GLENCORE v MSC*

One of the main problems of cyber-security is the very little number of cases in English Courts involving cyber-attacks. The lack of court cases leaves many important gaps and vacuums for regulating cyber-attacks. However, there is one actual case that could be interesting for the cyber-security perspective (Cybersecurity and Electronic Release Systems, 2018).

This case involved Glencore International AG v MSC Mediterranean Shipping Co SA. The litigation was about a cargo misdelivery claim using the electronic release system operating at Antwerp. At the port of Antwerp cargo is released using PIN codes instead of delivery orders. The claimant was a shipper Glencore International AG and the defendant was a carrier Mediterranean Shipping Co SA (Glencore International AG v. Mediterranean Shipping Co Sa, 2017).

According to the case, when the vessel arrived at the Port of Antwerp the defendant should have notified the agents at the port and after the bill of lading would have been presented. The notification included note that "containers will only be released against pincode". With the bill of lading's presentation defendant would release electronic document headed "Release Note", which gave a PIN code for

release of the cargo. The defendant released the PIN codes for the cargo, however, when the agents and their hauliers went to collect the cargo, they were already collected. Glencore proceeded with litigation for breach of contract, bailment and conversion.

According to the judgement of the English High Court the defendant (carrier) was held liable for delivering the goods to the unauthorized third party who hacked into the system by intercepting the PIN codes (Cybersecurity and Electronic Release Systems, 2018). During the trials it was presumed that the hackers infiltrated the carrier's computer networks and intercepted the PIN codes.

Defendant appealed and during the litigation process at the Court of Appeals they brought additional evidence that the hackers infiltrated into the networks of consignee and agents at the port of Antwerp and in this way gained the PIN codes. Nevertheless, the Court of Appeals still held the carrier liable because the carrier's bill of lading stipulated that the delivery of the cargo was to be made against delivery orders but the carrier had not issued them, the carrier's decision to deliver the cargo against the PIN codes was at it's own risk (Cybersecurity and Electronic Release Systems, 2018). The burden of proof was on MSC, however, they could not provide enough evidence.

This particular case shows how contractual relationships can potentially be sabotaged by the cyber-attack. In conclusion, this case illustrates that the carrier will bear the risk of loss or damage of cargo when using the electronic release system, unless it is expressly stated that electronic release system must be used, including the special terms about dealing with cyber-attacks (Glencore International AG v. Mediterranean Shipping Co Sa, 2017).

The above-mentioned case is fundamental, when the English Court of Appeals stated that the cyber-security clauses must be expressly articulated into the contractual relationship between the carriers, shipper and any other party. It should also be stated that the case also has potential vulnerabilities to criminal interference (Electronic Release System and Delivery of Cargo - MSC Mediterranean Shipping Company SA v Glencore International AG, 2017).

### *5.2. The Consequences of Cyber-Attacks*

In February 2017, hackers reportedly took control of the navigation systems of a German-owned 8,250 teu container vessel, en route from Cyprus to Djibouti for 10 hours (Blake, 2017). According to the report the vessel was paralyzed from the attack for 10 hours and its navigational systems was in complete control of hackers. It was also reported that the purpose of the attack was to navigate the ship into the trap of pirates. However, IT specialist was brought on to the vessel who installed the special applications to block the cyber-attack and the vessel was saved.

The exact way how the hackers entered through the system is unknown though it was reported that they had done it through maritime satellite communications - Inmarsat, Telenor, and Cobham. This particular incident raises several issues:

- A vessel could be hijacked by pirates;
- A vessel's cyber-attack could last longer periods;
- Only special expert in IT field was able to curb the attack;
- A vessel lost all navigational mechanisms to manoeuvre;
- Without navigational systems a vessel could sink (loss) with the cargo on board, the vessel could be damaged (hull), and the cost of loss of time to deliver the cargo.

In April of 2016, South Korea stated that around 280 vessels had to return to Korean ports after experiencing problems with their navigation systems, and claimed North Korea was behind the cyber-attack on the ships (Graham, 2017). According to the experts involved in the incident investigation, the cyber-attack was manipulated through GPS receivers on ships. Interesting facts lead the specialists to conclude that some GPS receivers were completely nonfunctional, but some were providing false information; according to the false information the vessels were in different territory.

From the marine insurance perspective analyzing the risks associated with this incident would be:

- Loss or Damage of a vessel (hull and machinery insurance);

- Loss of cargo (cargo insurance)
- Third party liability (P&I Insurance).

When analyzing both cases it is a very complicated field for insurers to enter into and insure the cyber-risks. Covering all the hull and machinery, cargo and P&I is impossible for now. The unique nature of cyber-attacks danger is its unpredictability and unknown consequences. The marine insurance industry will face tough realities when entering the cyber coverage.

### *5.3. Lloyd's of London*

An insurance market in London, adopted "Cyber-Attack Strategy" in 2016, which provides important insights into the contemporary perspective approaches of the insurance industry (Lloyd's Cyber-Attack Strategy, 2016). In 2015, the Lloyd's market wrote £322 million-worth of cyber policies, up from £206 million in 2014; in 2016, the number rose to £500 million. In just three years from 2013 to 2016, the number of Lloyd's syndicates writing cyber-risk went from 22 to 63.

According to analysts, the cyber insurance market will rise to $18 billion in 2025 (Lloyd's Cyber-Attack Strategy, 2016). The specialized cyber-insurance syndicates at Lloyd's market are insuring cyber-attack risk with (a) specific cyber insurance policies (covering risks such as breach response, liability, regulatory, extortion, business interruption, reputational harm) and (b) "Traditional" policies (e.g. property, marine, casualty) where cyber-attacks have the potential to cause a loss.

London's biggest insurance market, Lloyd's, is the leading industry covering cyber risks so far (Cyber Products at Lloyd's, 2018). On the market there are many special marine insurance companies which are providing special insurance policies against cyber risks. Lloyd's approach towards cyber insurance is rather structural and focuses on the harms that maybe affected by the assured, breach response, liability, regulatory, extortion, business interruption, and reputation harm.

### *5.4. P&I Clubs and Cyber-security: Coverage of Cyber Risks*

Among the experts of marine insurance there is an opinion that single marine insurance cannot cope with the growing threat from cyber-attacks and its best to deal with it with some kind of pool insurance (Marine Cyber Threat Causing Problems for T's & C's, 2018). According to the experts, the cyber-attack scenario can unfold through ECDIS which can contain 20 000 vessels, however, very few companies are updating the system and it could lead to a catastrophe for the whole shipping industry not only to marine insurance industry. The problem could be that ships cannot leave or enter the ports, or even worse if the ship where is in sea they will not be able to know where they are. The scope of a cyber-attack is yet unknown to most experts. Therefore, the risk that a single a marine insurance could not provide enough cover for such complex risk rises. Therefore, it is prudent to discuss marine cyber insurance in the context of P&I insurance.

The P&I Clubs, mutual association of shipowners and managers, are the biggest players in the insurance market. The International Group of Protection & Indemnity Clubs (IGPANDI) includes thirteen different clubs around the world. The clubs have their predefined rules and they incorporate special clauses in their insurance agreements.

The characteristics of cyber-attack on a vessel and the ultimate damage/loss it could lead to third-party liability. Protection & Indemnity (P&I) insurance covers shipowners for specific named risks. However, P&I insurance does not cover all possible risks or liabilities shipowner may be exposed and it is not comprehensive general liability coverage (Harter, 2003).

Most P&I Clubs of the Group have a sceptical approach towards the cyber-risks, which will be discussed further in this chapter. Almost all P&I Clubs incorporate a cyber-exclusion clause ("paramount clause"), Institute Clause CL380 (Osler, 2018). During this research, every rule book and circular was analyzed of all thirteen-member P&I Clubs from the International Group of Protection & Indemnity Clubs (IGPANDI).

This clause excludes any loss, damage, or liability caused either directly or indirectly by the use of a computer and its associated systems and software. The wording of the Clause gives specific definitions: *"... in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system."* (Institute Cyber Attack Exclusion Clause – Cl . 380, 2003).

In practice, if the loss, damage, or liability was caused either directly or indirectly by the use of a computer and its associated systems and software "as a means of inflicting harm," such loss, damage, or liability would be excluded from coverage (The Risk of Cyber Attack to the Maritime Sector, 2014). "A means for inflicting harm" can be interpreted as the cyber-attack specifically aimed at a vessel in order to harm or damage it. However, there is still the question what happens when "cyber-damage" is caused by an accidental failure. When a seafarer on the board injects a USB stick into the ship's computer and the whole ships system catches a "virus", does this scenario fall under that clause?

Another problem with the Cyber Attack Exclusion Clause is that in the UK it has not been tested at law (Mayle, 2018) and the interpretation of the clause is up to the insurers.

### 5.4.1. The Swedish Club:

The Swedish Club provides with "Notice of Cancellation, Automatic Termination of Cover, War, Nuclear etc. and Cyber Attack Exclusion Clause 2004-01-01 (W.1.3)" in their contracts regarding cyber-attacks. However, according to the Club the "Cyber Attack Exclusion Clause 2004-01-01 (W.1.3)", can be reinstated upon request (The Swedish Club Marine Insurance Update, 2018). The clause repeats the Institute Clause CL380 wording.

The Swedish Club in its rules (Rules for P&I Insurance Rules for FD&D Insurance Articles of Association 2018/2019, 2018) for P&I insurance implies also that "*Unless the Association otherwise decides there shall be no recovery from the Association in respect of liabilities, losses, costs and expenses arising from the use of any electronic trading system, other than a system approved by the Association, to the extent that such liabilities, losses, costs and expenses would not (save insofar as the Association in its sole discretion otherwise determines) have arisen under a paper trading system".*

Electronic trading systems could be used in the modern shipping industry for example electronic bills of ladings that are the vital instruments in international trading (Streat, 2018).

The Club incorporates Institute Clause CL380 and excludes liability caused by using paperless trading systems.

### 5.4.2. Japan P&I Club:

A claim arising out of a cyber-attack or cyber breach would be considered in the usual way with reference to the Rules (Japan P&I Club Rules 2018, 2018). When the cyber-attack would not fall under "war" or "act of terrorism" under the rule 35, a member's normal P&I cover will respond. The Club does not provide the land base cyber risk for the shipping companies. The Club considers that cyber-attacks affects mostly to Reputation damage, loss of IT equipment and economical loss. The fact that cyber-attack occurs is relied on official government releases and advices from IT experts.

Japan P&I Club divides cyber-risks into to two types: external factors and internal factors. External factors are unauthorized access, system hacking, viruses, social engineering. According to the Club internal factors are operational mistakes and general system failures (Cyber Risk and Cyber Security Countermeasures, 2018).

### 5.4.3.. Gard:

Gard incorporates Institute Cyber Attack Exclusion Clause – Cl . 380. and also excludes liabilities arising from electronic trading systems (Rules, 2018).

For P&I club Gard cyber is neither a named risk nor an excluded cause and therefore cover is not extended to cyber risks nor restricted for named risks where cyber is a cause. Some cyber-attacks may be defined as a war peril.

According to the Rules of the club Gard shall not be liable for any losses, liabilities, costs or expenses directly or indirectly caused by or contributed to or arising from the use or operation, as a means for inflicting harm, of any computer virus (Gard Rules 2018, 2018).

### 5.4.4. Standard Club:

According to the Clubs rules (P&I and Defence Rules and Correspondents, 2018) there is an exclusion relating to the paperless trading and incorporation of Institute Cyber Attack Exclusion Clause – Cl . 380. If a cyber-attack does not constitute "terrorism or another war risk" under risks exclusions, the Club will cover losses.

If, a cyber-attack were to be perpetrated by an individual or group for the purposes of causing general disruption and for no public cause, then this would be very unlikely (without more) to constitute terrorism for the purposes of the rules and a member's cover will respond in the normal manner. If a cyber-attack were targeted against a vessel by a government or organised rebels in a period of war or civil war, the war risks exclusion in the rules would come into force.

In the event that a cyber-attack does constitute 'terrorism', 'a hostile act by or against a belligerent power' or another excluded war risk, then the Club's excess P&I

War Risks clause may respond but not to the extent that the cyber-attack involves the use or operation of a computer virus as a means for inflicting harm (Banks, 2017).

### 5.4.5. Shipowners Club:

Shipowners Club retains the same practice of specific exclusions like most of the clubs. According to the Club's Rules (Shipowners Club Rules, 2018), computer virus coverage is excluded. The Club incorporates Institute Cyber Attack Exclusion Clause – Cl . 380. The exclusion includes also Chemical, Bio-chemical, Electromagnetic Weapons Exclusion Clause.

The Club is somewhat strict with its straightforward not covering policy. However, the Club has published several documents relating to cyber-security and hosted several webinars (The Shipowners' P&I Club Hosts Maritime Security Webinar – Recording Available, 2017).

According to the webinar hosted by the Club cyber risks are difficult to quantify for them, however, they also state that the variety of P&I claims with a cyber-element fall within cover. Also, according the webinar they are actively amending their policies for cyber cover.

The Club excludes liabilities, costs and expenses caused by usage of electronic paperless trading systems.

### 5.4.6. Britannia P&I:

According to the Club's rule books, there is no cyber-risk exclusion or even computer virus exclusion (Britannia P&I Protection and Indemnity Rules, 2018). The Club does not incorporate Institute Cyber Attack Exclusion Clause – Cl . 380.

During the research, the Clubs' rule books and circulars were analyzed. Britannia P&I does not provide any information about cyber-risks. The Club excludes cover of liabilities, costs and expenses caused by using paperless trading system, other than approved by the Club.

However, it is safe to assume that if liability caused by cyber-risk falls under P&I claims it will be covered according to the rules of the Club.

### 5.4.7. North P&I Club:

Still like other clubs North P&I Club excludes the losses and damages from the computer virus (P&I Rules, 2018). The North P&I Club only excludes the "computer virus", but not every liability arising from computer like is articulated in Institute Cyber Attack Exclusion Clause CL 380. The exclusion is part of war risks.

The P&I Club is still lacking in their rule books and policies any specific clauses related to the cyber-attacks. The Club excludes liabilities coming from electronic paperless trading systems.

North P&I Club was awarded with the UK's government backed scheme Cyber Essential's Plus accreditation in 2018 (North P&I Club Awarded with Cyber Essential Plus Accreditation, 2018) for implementing boundary firewalls and internet gateways, secure configuration, access control, malware protection and patch management.

### 5.4.8. Steamship Mutual

The Club incorporates the Institute Cyber Attack Exclusion Clause CL 380 (Rules 2018/2019, 2018).

The Club excludes the cover for liabilities, expenses and costs caused by the usage of electronic paperless trading systems.

### 5.4.9 The American Club

According to the rules of the American Club (By-Laws Rules List of Correspondents, 2018), it does not incorporate the Institute Cyber Attack Exclusion Clause CL 380. This is a rare example of a P&I Club, from International Group of Protection and Indemnity Clubs, which does not incorporate the Cyber Exclusion Clause.

Although the Club's rule book does not state any specific cyber-related risks or liabilities.

However, the Club excludes paperless electronic trading system liabilities.

### 5.4.10. West of England

The Club like above-mentioned clubs retains Institute Cyber Attack Exclusion Clause CL 380 (The Rules of Classes 1 & 2, 2018) and excludes paperless trading systems liabilities. The Club does not provide any other information regarding the cyber-risk

### 5.4.11. London P&I

The club incorporates the Institute Cyber Attack Exclusion Clause – CL. 380 (Class 5 the Protecting and Indemnity Rules, Clauses to Which Reference May Be Made in Certificates of Entry, 2018).

According to the rules, London P&I excludes liabilities caused by the usage of electronic trading system, similar to the other Clubs' paperless trading system exclusions.

Through the research no other additional information was obtained.

### 5.4.12. UK P&I Club

The UK P&I Club retains the same principle of work like other clubs and incorporates CL 380 Clause (UK P&I Rules, 2018).

The UK P&I Club excludes covering any liabilities, expenses and costs caused by electronic paperless trading system.

### 5.4.13 Skuld:

The club does not offer any coverages related to cyber security as of now. The company incorporates the same Institute Clause CL380 wording (2018 P&I Rules, 2018).

The Club excludes liabilities, expenses and costs caused by usage of electronic paperless trading systems.

## *5.6.. Obstacles and Problems the Marine Insurance Industry Faces*

Full incorporation of cyber-security clauses into the marine insurance agreements and policies has not happened this far. The marine insurance industry still lags behind the advancements of the cyber-attacks. There are not so many cyber-attacks directed on vessels and on shipping companies operating the vessels, but the numbers are definitely growing, Maesrsk and Cosco cases are examples. It is worth noting that in modern times there is no space left unchecked by hackers and cyber-criminals.

However cyber insurance can, therefore, be used to "plug the gaps" in cover which traditional insurance products leave behind, providing cover for a range of first-party and third-party losses that might arise as a result of an adverse cyber incident (Brasington & Hadwin, 2016).

Through the research a number of obstacles and impediments for the marine insurance industry in covering cyber-attacks were identified:

- Cyber-attack is very broad term that can be used in every industry, therefore, for particularly marine insurance usage "cyber-risk" must be specifically defined;
- The exact nature and characteristics of cyber-attack. The marine insurance industry, including P&I clubs provide many guidelines and circulars about raising awareness of the cyber-security, however, the exact nature of cyber-risk is still to be unknown to the industry;
- The scope of cyber-coverage. The exact scope what to cover is the problem for the marine insurance (The Business of Insuring Intangible Risks is Still in Its Infancy, 2018);
- There is no special clause introduced by clause underwriting leaders International Underwriting Association of London (IUA) and American Institute of Marine Underwriters (AIMU), except Cyber Attack Exclusion Institute Clause CL380;
- As discussed in this research earlier there is still uncertainties regarding the insurable interest in marine cyber-insurance;
- The relevance of the Marine Insurance Act 1906 and cyber-attacks as a marine risk.
- The lack of cases at courts of England and arbitrations. Major setback is little number of such cases. The case law development is essential for formulating the law of marine insurance regarding cyber-security.

Another problem for marine insurance in covering the cyber-risk is mitigation of loss. According to the mitigation doctrine the claimant must not unreasonably increase the loss suffered as a result of the breach (Gürses, 2017). With the increased

sophistication of cyber-attacks and their ever-changing nature it will be extremely hard for the assured to determine the actual loss and it could last long time to determine it. Especially when the data is stolen from a ship and the management of the ship is not aware what kind of data the hacker have stolen. Or maybe they only know that data was breached, however, they are not aware if hackers stole the data.

The burden of proof is another issue for marine insurance regarding cover of cyber-risks. The assured should provide evidence that cause of loss or damage (Gürses, 2017) was a cyber-risk. For example, if a vessel was attacked by the hackers and their refrigerators were turned off. This causes a complete loss of carried goods. However, after some time the hackers stopped attacking the vessel and refrigerators started working again normally. There is no trace left of the cyber-attack. How will the shipowner prove that it was cyber-attack?

### *5.7. Comparative Analysis of Cyber-Attacks and Other Marine Insurance Risks*

As cyber-attacks would play a major part in the marine insurance field in the future it is prudent to analyze what is the difference between "traditional", existing marine risks and cyber-risks. The grounds for comparison between marine risks and cyber-risks is to understand how the cyber-risks should be incorporated as a marine risk. Until now cyber risks are underestimated, however, the P&I Clubs, marine insurance companies, underwriters and legislators will absorb cyber-risks as one of the marine risks.

Section 3(2) of Marine Insurance Act 1906 states that:

"Maritime perils" means the perils consequent on, or incidental to, the navigation of the sea, that is to say, perils of the seas, fire, war perils, pirates, rovers, thieves, captures, seisures, restraints, and detainments of princes and peoples, jettisons,

barratry, and any other perils, either of the like kind or which may be designated by the policy.

The section provides a long list of marine risks to be applied in the marine insurance. Also at the end of section it articulates that *"…any other perils, either of the like kind or which may be designated by the policy"* which gives discretion to the contractual parties to draft their own risks into the policy.

Paragraph 7 of Marine Insurance Act 1906 provides that: The term "perils of the seas" refers only to fortuitous accidents or casualties of the seas. It does not include the ordinary action of the winds and waves.

"Perils of the seas" should be an unforeseen event that in a normal course of events could not happened and must be accidental (Gürses, 2017). Clause 2.1 of International Hull Clauses (01/11/03) is similar to the section 3(2) of Marine Insurance Act 1906 (Bennett, 2006). When analyzing the "perils of the seas" it is namely the risks associated with "the seas", however, in The Inchmaree case Lord Halsbury stated sea perils do not include those perils that arise from machinery which gives a vessel motive power to move. However, later the The Inchmaree Clause (Bennett, 2006) was developed as an extension to cover losses caused by hull, machinery, equipment, errors of navigation, etc, but it's not considered as a "peril of the sea" (Gürses, 2017). As for cyber-risks regarding marine insurance it should be noted that cyber-attack on a vessel which undertakes a voyage or adventure on the sea has similar characteristics as traditional marine risk. Thus, it could be assumed that cyber-attack on a vessel has a similar nature as The Inchmaree Clause, because it is an "additional perils clause" (Hodges, 1996).

Therefore, the nature of cyber-risk has a multi-dimensional character where, a cyber-attack could be comprehensive "peril" that could prejudice assured and it could (a) have a similar nature like peril of the sea in case of collision (Bennett, 2006); (b) have a similar result to The Inchmaree Clause like an explosion in the engine; (c) or could cause fire, ransom by pirates, rovers, thieves, be captured or seizured, be restrained or detained. The whole concept of a cyber-attack on a vessel draws very clear lines in similarity with the existing traditional marine risk in marine insurance.

## Chapter 6. Summary and Conclusion

Keith Alderman, the Associate Director of Lloyd's broker NDI Insurance, in his interview with IHS Fairplay noted that underwriters are reclusive because the volume of cyber loss and lack of information to base their pricing decisions (Cyber Security Threat Worries Marine Insurers, 2016). The problem with covering cyber-risks is not only the volume of cyber loss and pricing decisions, it is much greater and it is the lack of information about the ever-changing nature of cyber-attacks.

The research shows that insurers acknowledge the dangers of cyber-attacks, however, understanding the problem is the main issue, appraising the price of the exposure is the main barrier that stops the marine insurance industry to tackle the problem. Maritime companies are insisting too much on confidentiality and not declaring to the public if they have experienced cyber-attacks, because of the fear of losing clients, as well as decline in the stocks and are afraid to scare the shareholders.

The research shows that currently there are only two ways marine insurance responds to cyber-attacks: P&I insurance and special insurance policies.

The interviews were done during the research with P&I Club representatives (members of International Group of Protection & Indemnity Clubs), where the Clubs' stated that cyber-risks are considered as usual P&I risks and the Clubs will act according to the rule books. The information from the remaining Clubs, which did not respond to the interviews, was gathered through their official websites. According to the circulars and the rule books none of them provided cyber-risk insurance, except if the cyber-risk falls under usual P&I risk.

The P&I Clubs are excluding liabilities, expenses and costs caused by the usage of paperless electronic trading systems, other than that approved by the Club itself and the incorporating Institute Cyber Attack Exclusion Clause CL 380 (Cyber Risks and P&I Insurance, 2018). However, recently Lloyd's of London and the Prudential Regulatory Authority (PRA) of the UK are actively promoting that the Cyber Attack Exclusion Clause 380 is to be extended to include non-malicious attack (Marine Cyber Threat Causing Problems for T's & C's, 2018).

In 2016 IHS Fairplay and BIMCO conducted a cyber-security survey. According to the survey, only 11.7% of acknowledged attacks were notified to the company's insurers, where 3.3% of respondents said the loss had been covered by their insurer. From 3.3% none were paid through the hull and machinery policy, but less than 1% was covered by the P&I insurance. Only 1.9% had special cyber insurance (Cyber Security Threat Worries Marine Insurers, 2016).

Analyzing the current situation in the marine insurance industry regarding the cyber-risks, is like walking into a forest during the night without any guiding light and hoping that it will begin to be dawn soon. With much of uncertainty and confusion the marine insurance industry could take a reactive approach rather than a proactive.

## References

### Books:


Arnould, J., Gilman, J., & Merkin, R. (2008). Arnould's Law of Marine Insurance and Average (17th ed.). London: Sweet & Maxwell

Bennett, H. (2006). The Law of Marine Insurance (2nd ed.). New York, NY: Oxford University Press.

Gürses, O. (2017). Marine Insurance Law. New York, NY: Routledge.

Hodges, S. (1996). Law of Marine Insurance. London, UK: Cavendish Publishing Limited.

McNicholas, M. (2016). Maritime Security: An Introduction (2nd Ed.). Butterworth-Heinemann.

Marine Insurance. (2015). Institute of Chartered Shipbrokers. London, UK.

Soyer, B. (2001). Warranties in Marine Insurance. London, UK: Cavendish Publishing Limited.


### Articles:


Adamopoulos, A. (2018). Five Things to Watch: Regulation. Retrieved from https://lloydslist.maritimeintelligence.informa.com/LL1122214/Five-things-to-watch-Regulation

Andrews, W., & White. J. (2017). Digital Due Diligence: Four Questions to Evaluate Cyber Insurance Coverage. Retrieved from https://www.huntonak.com/images/content/2/7/v2/27753/Digital_Due_Diligence_Four_Questions_to_Evaluate_Cyber_Insurance.pdf

Banks, R. (2017). Cyber Risks and P&I Insurance Implications. Retrieved from http://www.standard-club.com/media/2533617/cyber-risks-and-pi-insurance-implications.pdf

Baker, J. (2018). Defending Shipping Against Cyber Crime. Retrieved from https://lloydslist.maritimeintelligence.informa.com/LL1124058/Defending-shipping-against-cyber-crime

Baker, James. (2018). Shipping Failing to Deal with Threat of Cyber Crime. Retrieved from https://lloydslist.maritimeintelligence.informa.com/LL1123453/Shipping-failing-to-deal-with-threat-of-cyber-crime

Blake, T. (2017). Hackers Took "Full Control" of Container Ship's Navigation Systems for 10 Hours. Retrieved from https://fairplay.ihs.com/safety-regulation/article/4294281/hackers-took-%E2%80%98full-control%E2%80%99-of-container-ship%E2%80%99s-navigation-systems-for-10-hours

Brasington, H. & Hadwin, S. (2016). Cyber Risks and the Maritime Industries: Risk Identification, Mitigation and Response. Retrieved from

http://www.nortonrosefulbright.com/knowledge/publications/137942/cyber-risks-and-the-maritime-industries-risk-identification-mitigation-and-response

Bueger, C. (2015). What is Maritime Security? Retrieved from https://ac.els-cdn.com/S0308597X14003327/1-s2.0-S0308597X14003327-main.pdf?_tid=50648997-8734-4101-b564-dc3b408689b3&acdnat=1535998841_f17f6d6df9860c3cb92cb702e9692191

Desjardins, J. (2017). Cybersecurity: Fighting a Threat That Causes $450B of Damage Each Year. Retrieved from http://www.visualcapitalist.com/cybersecurity-fighting-450b-damage/

Eling, M., & Hendrik Wirfs, J. (2016). Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class. Retrieved from https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf

Harter, S. (2003). Warranties and Exclusions in Protection & Indemnity Policies. Retrieved from http://micains.org/storage/sharter.htm

Hemsworth, M. (2018). The Fate of "Good Faith" in Insurance Contracts. Retrieved from https://www.i-law.com/ilaw/doc/view.htm?queryString=Carter+v+Boehm+&sort=date&sort=date&searchType=advanced-search&se=0&id=386470&searched=true

Mayle, T. (2018). Cyber Attacks Against Ships – Are You Covered? Retrieved from https://www.marsh.com/uk/insights/risk-in-context/cyber-attacks-against-ships.html

Moss, Jacques. (2018). How Will the Marine Insurance Industry Respond to New Sources of Risk?. Retrieved from https://knect365.com/shipping/article/593a4ff5-64bd-44a2-af7a-9806ee9e5f94/how-will-the-marine-insurance-industry-respond-to-new-sources-of-risk?utm_campaign=Share+Widget&utm_medium=Article+Share&utm_source=url

Myrvang, P. (2018). Countering Cyber Threats to Gas Networks. Retrieved from https://www.dnvgl.com/oilgas/perspectives/countering-cyber-threats-to-gas-networks.html?utm_campaign=OG_GLOB_18Q3_NEWS_Perspectives_08%7C2018&utm_medium=email&utm_source=Eloqua

Osler, David. (2018). Five Things to Watch: Marine Insurance. Retrieved from https://lloydslist.maritimeintelligence.informa.com/LL1122232/Five-things-to-watch-Marine-insurance

Rider, D. (2018). Cyber Security at Sea: The Real Threats. Retrieved from https://www.maritime-executive.com/blog/cyber-security-at-sea-the-real-threats#gs.KXvGw9I

Roche, Philip. (2016). Cyber Risk. *Stop Loss*, *1*6, 1-2. Retrieved from https://www.londonpandi.com/media/2025/5633stoploss67september.pdf

Schoenbaum, T. J. (1998). The Duty of Utmost Good Faith in Marine Insurance Law: Comparative Analysis of American and English Law. Journal of Maritime Law and Commerce 29(1), 1-40. Retrieved from https://heinonline.org/HOL/P?h=hein.journals/jmlc29&i=11

Shackelford, S. J.; Rusell, S. (2015). Risky Business: Lessons for Mitigating Cyber Attacks from the International Insurance Law on Piracy. Minnesota Journal of International Law 24(3), 1-15. Retrieved from https://heinonline.org/HOL/P?h=hein.journals/mjgt24&i=506

Shen, C. (2018). Cosco Shipping Targeted in Ransomware Attack. Retrieved from https://lloydslist.maritimeintelligence.informa.com/LL1123581/Cosco-Shipping-targeted-in-ransomware-attack

Streat, Simon. (2018). Electronic Bills of Lading Can Help Prevent Fraud or Deception. Retrieved from https://lloydslist.maritimeintelligence.informa.com/LL1123509/Electronic-bills-of-lading-can-help-prevent-fraud-or-deception

Textor, J. (2017). New OCIMF Pre-fixture Tanker Vetting Cyber Requirement. Retrieved from http://www.gard.no/web/updates/content/24478791/new-ocimf-pre-fixture-tanker-vetting-cyber-requirement

Allianz Risk Barometer 2018. (2018). Retrieved from https://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2018/

By-Laws Rules List of Correspondents. (2018). Retrieved from https://www.american-club.com/files/files/1819.pdf#page=32

Class 5 The Protecting and Indemnity Rules Clauses to Which Reference May Be Made in Certificates of Entry. (2018). https://www.londonpandi.com/documents/the-london-club-pi-rules-class-5-clauses/

Cyber Risks and Insurance In The Marine Industry. (2016) Retrieved from http://www.cambiasorisso.com/cyber-risks-and-insurance-in-the-marine-industry/

Cyber Risks and P&I Insurance. (2018). Retrieved from https://www.ukpandi.com/knowledge-publications/article/cyber-risks-and-p-i-insurance-142791/

Cybersecurity and Electronic Release Systems. (2018). Risk Watch – February 2018. Retrieved from https://britanniapandi.com/publication/risk-watch-february-2018/

Cyber risk and Cyber Security Countermeasures. (2018). Japan P&I Club Loss Prevention Bulletin. Retrieved from https://www.piclub.or.jp/wp-content/uploads/2018/05/Loss-Prevention-Bulletin-Vol.42-Full.pdf

Cyber Security Threat Worries Marine Insurers. (2016). Retrieved from http://edgegroup.com/cyber-security-threat-worries-marine-insurers/

Cyber Security Awareness. (2018). Retrieved from https://www.dnvgl.com/maritime/webinars-and-videos/videos/cyber-security-awareness.html

Cyber Security – Understanding Risk Simply. (2018). ABS. Retrieved from https://ww2.eagle.org/content/dam/eagle/publications/whitepapers/Cyber-Security-Understanding-RISK-Simply.pdf

Cyber Risks in Shipping. (2017). Retrieved from http://www.nepia.com/media/869527/Cyber-Risks-in-Shipping-LP-Briefing.PDF

DNVGL-RP-G108 Cyber Security in the Oil and Gas Industry Based on IEC 62443. (2018). Retrieved from https://www.dnvgl.com/oilgas/download/dnvgl-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html

Electronic Release System and Delivery of Cargo - MSC Mediterranean Shipping Company SA v Glencore International AG. (2017). Retrieved from https://www.steamshipmutual.com/publications/Articles/mscvglencore20170917.htm

Extreme Cyber-Attack Could Cost as Much as Superstorm Sandy. (2017). Retrieved from https://www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report

Four EU Cybersecurity Organisations Enhance Cooperation. (2018). Retrieved from http://ec.europa.eu/newsroom/informatics/item-detail.cfm?item_id=627791

Gard Rules. (2018). Retrieved from http://www.gard.no/Content/24908198/Rules_2018_web.pdf

Glencore International AG v Mediterranean Shipping Co SA. (2017). Retrieved from https://www.i-law.com/ilaw/doc/view.htm?id=382056#LLR:2017020186

Japan P&I Club Rules 2018. (2018). Retrieved from https://www.piclub.or.jp/attachment/insurance_guidebooks/2018%20Rules.pdf

Joint Industry Launches Latest Industry Guidelines On Cyber Security. (2017). Retrieved from https://www.bimco.org/news/press-releases/20170705_cyber-g

Lloyd's Cyber-Attack Strategy. (2016). Retrieved from https://www.lloyds.com/~/media/files/the-market/operating-at-lloyds/lloyds-cyber-attack.pdf

North P&I Club Awarded with Cyber Essential Plus Accreditation. (2018). Retrieved from http://www.nepia.com/news/press-releases-area/north-pi-club-awarded-with-cyber-essential-plus-accreditation/

P&I and Defence Rules and Correspondents. (2018). Retrieve from http://www.standard-club.com/media/2663541/pi-and-defence-rules-and-correspondents-201819pdf.pdf

P&I Loss Prevention Bulletin. (2018). Retrieved from https://www.piclub.or.jp/en/lossprevention/guide

P&I Rules. (2018). Retrieved from http://www.nepia.com/media/938888/NORTH-PI-Rules-2018-19-Full-online-v5-3-Sept.pdf

Rules for P&I Insurance, Rules for FD&D Insurance, Articles of Association 2018/2019. (2018). Retrieved from https://www.swedishclub.com/media_upload/files/Publications/TSC%20PI-FDD%20Rules_2018-19%20web.pdf

Rules 2018/2019. (2018). Retrieved from https://www.steamshipmutual.com/Downloads/Rules-and-Maps-/Club%20Rules/Steamship%20Interactive%20Rule%202018%202019.pdf

Steamship Mutual Chrterers Liability Cover. (2016). Retrieved from https://www.steamshipmutual.com/Downloads/Charterers/Steamship%20Mutual%20Charterers%20Liability%20Cover%20Overview.pdf

The Risk of Cyber Attack to the Maritime Sector. (2014). Retrieved from https://www.marsh.com/uk/insights/research/the-risk-of-cyber-attack-to-the-maritime-sector.html

The Rules of Classes 1 & 2. (2018). Retrieved from https://www.westpandi.com/globalassets/rulebook/2018.pdf

The Swedish Club Marine Insurance Update. (2018). Retrieved from https://www.swedishclub.com/media_upload/files/Additional%20insurance%202017/TSC%20Marine%20update.pdf

UK P&I Rules. (2018). Retrieved from. https://www.ukpandi.com/fileadmin/uploads/uk-pi/LP%20Documents/2018/RULES/2018_RULES_UKE.pdf

War Risks. (2018). Retrieved from http://www.nepia.com/media/926829/War-Risks-2018-19.pdf

2018 P&I Rules. (2018). Retrieved from https://www.skuld.com/contentassets/5cd37a56fa33442baec07c16ee4ac936/2018_skuld_rules.pdf

## Government Documents, International Conventions and other Legal Documents

Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation. (1988). Retrieved from http://www.admiraltylawguide.com/conven/suppression1988.html

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union. (2016). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1533418187256&uri=CELEX:32016L1148

IMO Guidelines On Maritime Cyber Risk Management. (2018) Retrieved from http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC.1-CIRC.1526%20(E).pdf

Institute Cyber Attack Exclusion Clause – Cl . 380. (2003). Retrieved from https://www.modernaforsakringar.se/siteassets/documents/foretag--industri/villkorsbanken/foretagsforsakring/allmanna-villkor/transport/institute-cyber-attack-exclusion-clause---cl-380-vst-24-1-.pdf

ISO/IEC 27000 Family - Information Security Management Systems. (2018). Retrieved from https://www.iso.org/isoiec-27001-information-security.html

Marine Insurance Act 1906 (revised version). (2018). Retrieved from http://www.legislation.gov.uk/ukpga/Edw7/6/41/contents

National Strategy for Maritime Security. (2014). Retrieved from https://www.gov.uk/government/publications/national-strategy-for-maritime-security

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). (2018). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1535246401086&uri=CELEX:02016R0679-20160504

Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. (2017). Retrieved from http://www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution%20MSC.428%2898%29%20-%20Maritime%20Cyber%20Risk%20Management%20in%20Safety%20Management%20Systems.pdf

SOLAS XI-2 and the ISPS Code. (2018). Retrieved from http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

The Guidelines on Cyber Security Onboard Ships. (2017). Retrieved from http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

## Additional Sources

Graham, L. (2017). Shipping Industry Vulnerable to Cyber Attacks and GPS Jamming. Retrieved from https://www.cnbc.com/2017/02/01/shipping-industry-vulnerable-to-cyber-attacks-and-gps-jamming.html

Marine Cyber Threat Causing Problems for T's & C's. (2018). Retrieved from https://insurancemarinenews.com/insurance-marine-news/marine-cyber-threat-causing-problems-for-ts-cs/

McArdle, M. (2018). Should Paying Even a Paltry Ransom to Hackers be a Federal Crime? Retrieved from https://www.washingtonpost.com/blogs/post-partisan/wp/2018/03/30/should-paying-even-a-paltry-ransom-to-hackers-be-a-federal-crime/?noredirect=on&utm_term=.2a58a5f15a5a

Morris, D. (2018). Chinese Hackers Steal Sensitive Data on U.S. Subs and Missiles from Military Contractor, Report Says. Retrieved from http://fortune.com/2018/06/10/chinese-hackers-steal-sensitive-data-us-military/

The Business of Insuring Intangible Risks is Still in its Infancy. (2018). Retrieved from https://www.economist.com/finance-and-economics/2018/08/25/the-business-of-insuring-intangible-risks-is-still-in-its-infancy

What are the Five Principles of Marine Insurance? (2018). Retrieved from https://securenow.in/insuropedia/five-principles-marine-insurance