UNIVERSITY OF CAPE TOWN - FACULTY OF LAW

NAME : TILLY SEBOKO

STUDENT NO: SBKGOI003

SUPERVISOR: ASSOCIATE PROFESSOR GRAHAM BRADFIELD

QUALIFICATION: MASTER OF LAWS BY COURSEWORK AND MINOR DISSERTATION

SUBMISSION DATE: 10 FEBRUARY 2020

OFFSHORE CYBER RISK IN THE MARINE INDUSTRY: LIMITATIONS AND CHALLENGES FACED BY THE INSURERS AND POLICYHOLDERS

Contents

CHAPTER 1: INTRODUCTION

Introduction & Background

As stated by Stephen Harris, a mere 30 years ago, the idea of commercial cyber-attack was rather a topic for the science fiction novelists than reality.'[1] However, nowadays we witness a growing tendency of reoccurrence of this phenomenon across many sectors that rely on progressively advancing technology. Despite always being known as a conservative field, the maritime industry is no exception in terms of the exposure to risks that result from cyber-attacks.

For decades, the commercial ships relied on radio telecommunication for navigation purposes, however, just like the most of the industries, also maritime is evolving and towards digital transformation.[2,3] This era has brought many benefits, but simultaneously also new risks and challenges for ships (i.e. offshore) and ports (i.e. onshore), as new tools get continuously implemented across various business areas.

It is no secret that the ships and ports are becoming increasingly dependent on the information technology for both, onshore and offshore operations[4], and therefore also progressively prone to cyber risks, which represent a threat to the entire digital world.[5]

As implied above, the Cyber risk or the damage resulting from cyber-attack is an emerging danger that continues to evolve alongside with the tech advancements. It encompasses complex challenges that the shipping industry (i.e. ship-owners and the insurance market) is not prepared to prevent or manage. The cyber-attacks are seen to cause an unforeseen extent of financial

[1] Jacques Moss 'How will the Marine Insurance Industry Respond to New Sources of Risk?' *Maritime, Legal, Regulation and Insurance* 11 May 2018, available at *https://knect365.com/shipping/article/593a4ff5-64bd-44a2-af7a-9806ee9e5f94/how-will-the-marine-insurance-industry-respond-to-new-sources-of-risk,* accessed on 25 August 2019.

[2] Amitava Chakrabarty 'What Marine Communication Systems Are Used in the Maritime Industry?' *Marine Insight 22 November 2019*, available at *https://www.marineinsight.com/marine-navigation/marine-communication-systems-used-in-the-maritime-industry/,* accessed on 02 January 2020.

[3] Cyber Risk Management Project *CyRiM Report 2019 Bashe* 'Attack Report - Global infection by contagious malware' 10 January 2019 at 2, available at *https://www.financialinstitutionslegalsnapshot.com/wp-content/uploads/sites/161/2019/02/CyRiM-report.pdf,* accessed on 20 December 2019.

[4] Allianz Global Corporate & Specialty 'Safety and Shipping Review 2017: An annual review of trends and developments in 'shipping losses and safety at 34, available at available at *https://www.agcs.anz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Safety-Shipping-Review-2017.pdf,* accessed on 05 January 2019.

[5] Baltic International Maritime Council 'The Guidelines on Cyber Security on Board, Version 3.0' *BIMCO* at 13, available at *http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16,* accessed on 20 July 2019.

damage, which led the marine insurance companies to incorporate several devices, which limit their liability for damage protecting the business from the risk of bankruptcy.[6]

As much as this can be beneficial for the insurers, this has left a significant marine insurance gap, also known as underinsurance, as the exclusion of the cyber risk instances is meant to preclude the coverage. The author of this dissertation is of the view that the primary goal should be to minimize the cyber risk by filling the insurance gap, while establishing an acceptable solution for the insurers as well as the insured in a form of lowered risk and affordable premiums.

It is essential to realize that any disruption of the shipping logistics and transportation system could cause serious damage and billions of dollars in financial loss, since the shipping industry contributes to 90% of the global economy through goods carried by sea;[7] involving some 60,000 merchant ships.[8] Hence, it is important that cyber risks are eliminated in order to avoid any economic commotions which would significantly affect the global trade.

Besides the mentioned technological advancements, the increase in occurrence of cyber risks was also contributed to by the introduction of Regulation 19 of SOLAS Chapter V [9], as it requires the vessels to operate on new technological navigation systems; e.g. AIS, GPS, etc.
Since then, the vessels have become more vulnerable and susceptible to hacking and cyber-attacks are more common due to increased dependence on technology and remote access respectively.[10] According to Malik *et al*. the containerships appear to be more prone to be targeted, due to their apparent commercial value and constant offshore presence, which can be illustrated on numerous cyber incidents taking place in recent years. [11]

---

[6] Regulation (EC) No 392/2009 of the European Parliament and of the Council of 23 April 2009 on the liability of carriers of passengers by sea in the event of accidents, available at *https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009R0392*, accessed on 22 January 2020.

[7] International Maritime Organisation (IMO) 'Human Element', available at *http://www.imo.org/en/OurWork/HumanElement/Pages/Default.aspx,* accessed on 11 January 2020.

[8] Allianz Global Corporate & Specialty 'Cyber Transparency and Risk Management' available at *https://www.agcs.allianz.com/news-and-insights/reports/shipping-safety.html*, accessed on 12 October 2019.

[9] International Maritime Organisation 'SOLAS (Safety of Life at Sea) chapter v safety of navigation' published on 1 July 2002 , available at *http://www.imo.org/en/OurWork/Facilitation/Documents/SOLAS%20V%20on%20Safety%20of%20Navigation.pdf*, accessed 11 January 2020.

[10] Julian Clark 'The Changing Face of Maritime Law and Risk – Cyber, E-Commerce, Automation of Vessels': Maritime 2019' in *International Comparative Legal Guides 2019*, ICLG.COM 30 July 2019, available at *https://iclg.com/practice-areas/shipping-laws-and-regulations/2-the-changing-face-of-maritime-law-and-risk-cyber-e-commerce-automation-of-vessels*, accessed on 9 September 2019.

[11] Malik Shahzad Kaleem Awan and Mohammed A. Al Ghamdi 'Understanding the Vulnerabilities in Digital Components of an integrated Bridge System (IBS)' (2019) 7 *MDPI (Journal of Marine Science and Engineering)* at 350, available at *https://doi.org/10.3390/jmse7100350*, accessed on 16 November 2019.

In 2016 alone, nearly 300 ships were ordered to return to their port of origin, because of their navigation system being infiltrated, and as a result, the vessels transmitted false navigation information.[12] Similarly, in June 2017, at least 20 ships had their GPS navigation hacked in the Black Sea region. This not only led to their spoofing and subsequent return to the port until the problem was fixed, but also resulted in shipment delays and therefore significant commercial losses.

Besides other, this study will show that incidents like this expose shipowners to significant financial risk, which is further intensified by the already mentioned insurance gap, as such business disruptions represent a significant risk to shipping companies.[13] Likewise, should a major cyber-attack be a subject to insurance cover of a single underwriter, it may lead to significant financial toll and potentially result in bankruptcy of the insurer, which demonstrates how complex this issue really is.

It is clear that cyber-risk is now a new form of piracy,[14] in the sense that the modern pirates perpetrate their attacks or robberies in a modernized way by using technology. Such analogy is not far from reality as the pirates have always been known for taking over vessels on the high sea by boarding on the ship, while recently, they have become technologically savvy, skilled and innovative, as they execute their plan by not boarding on the ship but rather by hacking navigation system of the vessel.[15]

Scope of the dissertation

It will be argued that, as with all indemnity insurance covers, pricing insurance cover at reasonable and competitive levels requires accurate assessment and comprehensive management of these risks. The dissertation will also explore how insurers can deal with such virtual threats through

[12] Julian Clark 'The Changing Face of Maritime Law and Risk – Cyber, E-Commerce, Automation of Vessels': Maritime 2019' in *International Comparative Legal Guides 2019*, ICLG.COM 30 July 2019, available at *https://iclg.com/practice-areas/shipping-laws-and-regulations/2-the-changing-face-of-maritime-law-and-risk-cyber-e-commerce-automation-of-vessels*, accessed on 9 September 2019.

[13] Dana Goward 'Expert Opinion: Spoofing attack reveals GPS vulnerability' *GPSworld 18 July 2017*, available at *https://www.gpsworld.com/expert-opinion-spoofing-attack-reveals-gps-vulnerability/*, accessed on 11 November 2019.

[14] Luke Graham 'The new face of piracy: cybercrime is threatening the shipping industry' *CITA.M.* 26 November 2018, available at *https://www.cityam.com/new-face-piracy-cyber-crime-threatening-shipping-industry/*, accessed on 25 August 2019.

[15] Ibid.

gathering and use of the historical information as well as those obtained from the insured. Likewise, it will be suggested that insurers should utilize the contractual tools already available to them, in order to manage the risks and control the level of their liability exposure.

In line with the aim of the dissertation defined below, the study will describe how the marine insurers handle the challenges of cyber risks and provide critical recommendations on how such matters shall be dealt with in the future. Subsequently, the author will justify these suggestions and describe what makes them more appropriate over others. Given the fact that this paper focuses on relatively emerging risk which is likely to demand a suitable insurance cover, the goal is to elaborate on how this cover should be provided rather than if at all.

Many academics and legal researchers have written on cyber-attacks and cyber awareness; however, nothing has been written on the challenges faced by the insurers in providing insurance cover against cyber risks. The dissertation will therefore also elaborate on the issued guidelines that serve as a preventative measure for the cyber risk management and compare the existent insurance products based on their relevancy in relation to the discussed insurance gap.

Lastly, the author will portray a view on how the identified underinsurance may be eliminated or at least reduced when insurers see benefit in providing cover against such risks; i.e. once they are confident in managing their levels of exposure to liability for claims relating to losses arising from the materialization of cyber-attacks.

Aim of the dissertation

The aim of this dissertation is to consider how marine insurers and policyholders can deal with the challenges presented by cyber risks, contributing to reasonably priced marine insurance cover. Concurrently, the goal of this paper is to generate possible ways of how to manage the identified cyber risks and subsequently formulate recommendations to eliminate the suggested insurance gap by offering an affordable premium pricing.

Structure

Chapter 1:

As seen above, this section serves as a rather introductory part, where author familiarizes the reader with background, scope and aim of the dissertation. At the end of this chapter the author also

elaborates on the structure of the paper to introduce the order in which she presents the distinct subjects.

Chapter 2:

This part of the dissertation serves to define terms used in the dissertation in order to provide the reader with better understanding of the context. It also illustrates the severity of the cyber-attacks on the past incidents, in order to illustrate its potential in terms of the financial damage and risk exposure. Furthermore, this chapter will also highlight various ways in which are cyber-attacks perpetrated in maritime industry and include the discussion related to implications of such events. Lastly, the author unpacks the losses related to these incidents in order to demonstrate the extent of damage inflicted thereby, highlighting the attention that this topic deserves.

Chapter 3:

This section will discuss ways of dealing with the cyber risk management and how to conduct damage control resulting from cyber-attacks. Furthermore, this chapter also elaborates on various guidelines and framework order to establish how these can be used to assess and manage the cyber risks faced by insurers and the insured.

Chapter 4:

This chapter focuses on the cyber risk challenges in the maritime sector, as viewed from the perspective of both – the insurer and the insured. It further elaborates on the type and extent of the damage, potentially caused by these challenges to provide a better understanding of their repercussions. Lastly, this section also attends some of the challenges faced by the policymakers, in order to demonstrate the complexity of cyber risk implications on the maritime industry.

Chapter 5:

This part of the dissertation focuses on the insurers approach to cyber risk in marine sector. In this part, the attention is given to the pre-contractual and contractual tools that can be used to protect the insurer as well as the insured and elaborates on definitions of these measure. The discussed components include the terms that can be incorporated in the phase of policy drafting.

Chapter 6:

This section of the paper examines and compares various cyber insurance covers. Here, the author selects a variety of products that intended to fill the existent insurance gap in the shipping industry. Furthermore, this chapter will also look at the similarities and differences of these policies in order to seek an existent clause that would be affordable and eligible for the future upgrade.

Chapter 7:

This conclusive section of the dissertation will summarize the findings of the paper and refer back to the aim of the study, set out within the chapter 1. Additionally, it will also define recommendations that will be of significant use to the insurers and the insured, aiding to mitigate the cyber risk while suggesting the ways to offer an affordable cyber risk cover.

CHAPTER 2: CYBER RISK IN MARITIME INDUSTRY: ITS IMPLICTIONS ON LAW AND INSURANCE SECTOR

Definitions

As stipulated in Chapter 1, the cyber risk is an increasingly re-occurring threat that significantly affects the global economy and those that participate in its various sectors.[16]

To illustrate the above, the 2018 World Economic Forum's Global Risk Report presented cyber-risks as one of the top five risks, as identified by the experts and decision-makers across the globe. According to Allianz Risk Barometer published later the same year, the cyber incidents ranked number two, representing a potential business operations interrupter for 40% of the respondents, moving up this ranking from fifth place in 2015, when identified as a potential concern by 17% of the businesses.[17]

The following year, the Global Maritime Forum unsurprisingly aligned with the above indicated results, as the International Union of Marine Insurance (IUMI), published a Global Maritime Issues Monitor 2019, where cyber-attack and theft appeared as one of the top five issues and risks confronted by the maritime industry worldwide.[18]

Just to put the above into financial perspective, the 2019 Lloyd's of London report shows that severe cyber-attack could cost the global economy more than $120bn, which is comparable to the damages caused by the major natural disasters, such as hurricane Katrina or Sandy. The report also points out the globally growing insurance gap caused by the increasing occurrence of cyber-crime, as there seems to be a lack of cover options, calling for innovations in risk assessment and premium designs with the situation being no different in the maritime industry. As we investigate these various reports, it is indisputable that cyber-risks will not come to an end anytime soon. Instead, it is obvious that cyber-attacks on ships and port operation systems are here to stay, and

[16] Swiss Re 'From emerging risk to core business: cyber attacks', available at https://www.swissre.com/about-us/corporate-responsibility/risk-intelligence/emerging-risks/case-study-cyber-attacks.html, accessed on 18 December 2019.

[17] Allianz Global Corporate & Specialty 'Allianz Risk Barometer 2019 top 10 threats' *https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019-Top10.pdf,* accessed on 20 December 2019.

[18] Marsh 'Global Maritime Issues Monitor 2018' available at 34 *https://www.marsh.com/uk/insights/research/global-maritime-issues-monitor-2018.html*, accessed on 30 November 2019.

the shipping industry needs to develop a sustainable solution soon from the prevention, risk management and insurance perspective likewise.[19]

Cyber-crime and cyber attacks

There is currently no standardised definition of 'cyber risk'.[20] However, it can be argued that cyber-risk is a consequence of unlawful conduct carried out by means of computers to disrupt one's business operations. For present purposes a definition of cyber-risk as 'any risk of accidents, incidents, financial loss, business disruption or damage to the reputation of an organization through a failure of its electronic systems or by the persons using those systems', will be adopted.[21]Cyber-attack is an adverse consequence of cyber risk. It can be defined as 'Attempts to damage, disrupt, or gain unauthorized access to computer, computer system, or electronic communication network. An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of data or stealing controlled information.[22]

Cyber incidents

Cyber incidents can be defined as events that 'is an occurrence, which actually or potentially results in adverse consequences to an onboard system, network and computer or to the information that they process, store or transmit, and which may require a response action to mitigate the consequences.[23]

[19] Lloyd's Register 'Tackling an evolving threat' available at https://www.lr.org/en-za/cyber-security/, accessed on 20 December 2019.

[20] International Association of Insurance of Insurance Supervisor(IAIS) 'Issue Paper on Cyber Risk to the Insurance Sector' August (2016) at 5, available *at https://www.iaisweb.org/file/618957/issue-paper-on-cyber-risk-to-the-insurance-sector*, accessed on 21 November 2019.

[21] North of England P& I Association 'Cyber Riskin Shipping: Loss Prevention Briefing for North Member' available on *http://www.nepia.com/media/869527/Cyber-Risks-in-Shipping-LP-Briefing.PDF,* accessed on 29 August 2019.

[22] FFIEC 'Cybersecurity Assessment Tool Glossary' published on 1 June 2015, available at *http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_C_Glossary_June_2015_PDF5.pdf,* accessed on 02 September 2019.

[23] Baltic International Maritime Council 'The Guidelines on Cyber Security on Board, Version 3.0' *BIMCO* at 50, available at *http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16,* accessed on 20 July 2019.

Cyber Attacks in maritime industry

As mentioned in the definition of the cyber-attacks listed within this chapter, such incidents represent an "unauthorized access" to the third party's system or communication. This, when translated into context of maritime industry and its offshore operations respectively, stands mostly for the attempts to disrupt the navigation systems based on the vessel communication; i.e. sent and received data. In order to understand the implications of cyber-attacks on the ships, it is therefore useful to elaborate a bit more on some of the vessels 'communication systems that represent a target for cybercrime.

In 2000, the International Marine Organization (IMO) published *Guidelines for the Installation of a Shipborne Automatic Identification System (AIS)*,[24] which required that AIS be fitted on all passenger ships as well cargo international vessels with 300+ tonnage and local voyages of 500+ tonnage, as of 2004.[25] These AIS Guidelines require ship owners to install AIS that is capable of automatically exchanging navigation information in order to detect a possible danger on the sea, providing the vessels' masters with the ships' identity, type, position, course, speed, and navigational status. In addition, the system has to be able to transmit accurate safety information to other sailing ships and ports to avoid collision and to possibly help a fellow ship in case of emergency.[26] The idea for installing the fitted AIS is to create navigation platform on the sea that would make the communication between vessels much more inclusive and therefore efficient. Besides the AIS, the IMO also requires ships to possess other navigational systems - namely Global Positioning System (GPS) and Electronic Chart Display and Information System (ECDIS) in order to increase the layers of accuracy and security. [27]

While GPS, which is part of Global Navigation Satellite System (GNSS), works on the basis of communication with the satellite where position, speed and course of the ship are taken into

[24]International Maritime Organisation 'AIS transponders' 6 June 2003,available at *http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx,* accessed on 09 September 2019.
[25] Ibid.
[26]Marsh 'Cyber Gap Insurance Cyber Risk: Filling the Coverage Gap' at 2, available at *www.oliverwyman.com/content/dam/marsh/Document/PDF/UKen/CyberGapInsuranceCyberRiskFillingtheCoverage,* accessed on 07 December 2019.
[27]International Maritime Organisation 'AIS transponders' 6 June 2003,available at *http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx,* accessed on 09 September 2019.

consideration in order to determine the trajectory and time it is going to take to reach its pre-set destination, ECDIS is an alternative to nautical charts. [28]

Since the installation of AIS, ECDIS, and GPS on ships there has been indisputable increase in security as suggested above. However, such implementation also means an increase in reliance on technology and therefore growing likelihood of attempted cyber-attacks.[29] In other words, these technological navigation devices led vessels to be dependent on them and, as a result, the ships have become more prone to cyber-risks, placing them at a higher chance of being spoofed, and their navigation system infiltrated or hacked.[30]

As for GNSS and GPS in particular, these are often subjected to the cyber activity with negative intent due to their influence on the navigation of the ship, as these satellite-based technologies advise the crew on the right course.[31] Once manipulated, the suggested direction of the ship may be misleading as a result of the invasion and subsequent deliberate amendment of the vessel coordinates.[32]

On the other hand, AIS is designed as a tool that can transmit navigation information about the ship to other ships, the master and the pilot automatically.[33] When it comes to AIS, on the other hand, this system of navigation determines the ship's current location (similarly to GPS), however, it also suggests the vessel's identity, surrounding traffic as well as other details related to the carrier.[34] Once again, such information can be misused and prepare the ground for criminal activity; e.g. hijacking or heist.

Cybersecurity

[28] Ibid.
[29] Ibid.
[30] Ibid.
[31] Arunabha Mukhopadhyay, Samir Chatterjee, Debashis Saha et al 'Cyber-risk decision models: To insure IT or not?' Decision Support System 56 (2013) 11-26 at 1.
[32] Lloyds Register 'LR Warns of the Risks Associated with Marine Information Technology' available on *https://www.lr.org/en/latest-news/lr-warns-of-the-risks-associated-with-marine-information-technology/*,accessed on 20 August 2019.
[33] Ibid.
[34] Cambiaso Risso Group 'Cyber Risks and Insurance in the Maritime Industry' available at *http://www.cambiasorisso.com/cyber-risks-and-insurance-in-the-marine-industry/* accessed on 25 August 2019.

Cyber security may be defined as, '[t]he collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and an organisation and user's assets.'[35]

Examples of cyber-attacks and their frequency

To demonstrate the above on the actual example in order to achieve a better understanding, the author decided to list few examples of cybercrime incidents that significantly affected some of the major careers around the world.

In April 2016, South Korea noted over 280 vessels having to return to its ports of origin after experiencing navigational problems at the sea, while sailing. It was later alleged that North Korea was behind these cyber-attacks which caused the ships' GPS signal to be jammed, leading to some of the vessels' signal to deteriorate while others received a false signal resulting in navigational issues also known as spoofing.[36] In June 2017 the Black Sea region experienced a very similar problem of GPS jamming. In this instance, about 20 vessels had to return to their port of origin as the spoofed GPS showed the current location to be the Geldendzhik airport, about 25 miles away from the Black Sea.[37]The same year, another container ship heading from Cyprus to Djibouti was attacked by the so-called cyber pirates, where the hackers infiltrated the navigation system of the vessel and thereby gained a full control of the ship for a period of 10 hours. This caused the captain to be unable to maneuver the ship and the problem had to be resolved by an IT expert. It is alleged that the attackers intended to direct the vessel to a location where they would be able to board on to it, in order to commit a physical robbery act potentially even hijacking the vessel.[38] Even though

[35] Lloyds Register 'Cyber safe for marine,' available at https://www.lr.org/en/cyber-safe-for-marine/, accessed on 15 September 2019.

[36] Luke Graham 'Shipping industry vulnerable to the cyber-attacks and GPS jamming' 1 February 2017,available at *http://www.cnbc.com/2017/02/01/shipping-industry-vulnerable-to-cyber-attacks-and-gps-jamming.html,* accessed on 18 November 2019.

[37]The Maritime Executive 'GPS Spoofing Patterns Discovered' available at *https://www.maritime-executive.com/article/gps-spoofing-patterns-discovered*, accessed on 18 November 2019.

[38] Tanya Blake 'Hackers took 'full control' of the ship's navigation systems for 10 hours' available at *https://www.asket.co.uk/single-post/2017/11/26/Hackers-took-full-contol-of-container-ships-navigation-systems-for-10-hours-AketOperations-AsketBroker-Elousiv-IHS4SafetyAtSea-TnyaBlake-cybersecurity-piracy-shipping,* accessed on 18 November 2019.

these malicious intents did not turn into reality, it is clear that the incident resulted in delayed voyage, caused reputational as well as financial damages.[39]Last example of the cybercrime that illustrates the power of hackers for the purpose of this dissertation is related to Maersk – the largest container shipping company controlling 18% of the sea transport market. [40] It all began when an employee in Ukraine replied to an email unaware that it contained, the so-called, NotPetya virus.[41] On the 17 June 2017, the hackers used the previously achieved infiltration of the company's system and targeted Maersk's headquarters in Copenhagen, Denmark. In turn, the already established presence of the virus led to a massive business disruption affecting Maersk's facilities, resulting in the suspension of quite a few its port terminals.[42]

Maersk's business interruption resulted in failure to take new orders and all their daily operations were affected.[43] The suspension majorly affected USA, Spain, India, Netherlands and other countries.[44] The cyber-attack left the container shipping, port and tug operations, oil and gas production, drilling services and oil tankers inoperative.[45] In addition, there was a ransomware attack demand in return of their files.[46] The hacking resulted in Maersk losing at least $200-300 million in revenue, costs of fixing its IT system, costs of 45 000 computers that were affected and needed to be replaced, financial loss incurred on upgrading and a new IT system installation,

[39] David Miranda Silgado *Cyber- attacks: a digital threat reality affecting the maritime industry* (unpublished LLM Worlds Maritime University Dissertation, 2018) at 32, available at *https://commons.wmu.se/cgi/viewcontent.cgi?article=1662&context=all_dissertations*, accessed on 23 July 2019.

[40] Dromo Bureau of Shipping 'Guidelines on Maritime Cyber Risk Management' available at *https://maritimecyprus.files.wordpress.com/2018/11/dromon-guidelines-on-maritime-cyber-risk-management.pdf*, accessed on 04 December 2019.

[41] Jonathan Saul 'Cyber threats prompt return of radio for ship navigation' available at *http://www.reuters.com/article/us-shipping-gps-cyber/cyber-threats-prompt-return-of-radio-for-ship-navigation-idUSKBN1AN0HT,* accessed on 19 November 2019.

[42] David Miranda Silgado *Cyber- attacks: a digital threat reality affecting the maritime industry* (unpublished LLM Worlds Maritime University Dissertation, 2018) at 45, available at *https://commons.wmu.se/cgi/viewcontent.cgi?article=1662&context=all_dissertations*, accessed on 23 July 2019.

[43] Dromo Bureau of Shipping 'Guidelines on Maritime Cyber Risk Management' available at *https://maritimecyprus.files.wordpress.com/2018/11/dromon-guidelines-on-maritime-cyber-risk-management.pdf*, accessed on 04 December 2019.

[44] Ibid at 45.

[45] Julian Clark 'Cybercrime in the shipping industry: An overview of the risks and how they apply to you' *MLASA* 2 September 2018,at available at *http://www.mlasa.co.za/wp-content/uploads/2017/09/Cyber-crime-in-shippinh-Julian-Clark.pdf,* accessed on 19 November 2019.

[46] Ibid.

financial loss for replacing 40 000 servers and additional losses due to opportunity cost caused by this business disruption.[47]

It is now clear that cyber-attacks in maritime industry appear in a frequent incidence posing a substantial risk, which is, mainly due to its complexity and extent, difficult to assess. Meantime, such events represent a challenge from the perspective of prevention as well as liability, demonstrating the previously discussed insurance gap and its scope respectively. The tools and ways the insurers deal with such challenges are to be further discussed in the chapter 4 where the author elaborates on the limitations that the insurers (as well as the insureds) face.

Maritime Law

Peril of the sea

The section 3(2) of the Marine Insurance Act 1906, defines Maritime Perils as 'the perils consequent on, or incidental to, the navigation of the sea, that is so say, perils of the sea, fire, war perils, pirates, rovers, thieves, captures, seizures, restraints, and detainments of the princes and peoples, jettisons, barratry, and other perils, either of the like kind or which may be designated by the policy.' Furthermore, schedule 8 of Rules for Construction of Policy define Peril of the sea a 'fortuitous accidents or casualties of the seas. It does not include the ordinary action of the winds and waves.'[48] It is important to define peril of the sea as focus of this dissertation i.e. hacking of the navigation of the system of the constitute a peril of the sea risk.

Marine Insurance

Marine insurance claims are governed by the Marine Insurance Act 1906.[49] Cyber risk is currently not regulated by the Marine Insurance Act nor subject to the Standard Form contract.

[47] David Miranda Silgado *Cyber- attacks: a digital threat reality affecting the maritime industry* (unpublished LLM Worlds Maritime University Dissertation, 2018) at 33, available at *https://commons.wmu.se/cgi/viewcontent.cgi?article=1662&context=all_dissertations*, accessed on 23 July 2019..

[48] Section 3(2) of the Marine Insurance Act 1906; Schedule 7 of the Marine Insurance Act 1906, Schedule Rules for Construction of Policy.

[49] Section 1 of the Marine Insurance Act 1906.

Cyber risk contracts are currently regulated by the general law of contract. This chapter deals with cyber risks within the context of the Marine Insurance Act 1906; aiming at aligning the risks with the Act. This chapter will make an argument on how cyber risks should be treated as marine insurance peril; and how cyber risks contract should conclude using the general principles of a contract of the Marine Insurance Act. Subsequently, add pre-contractual/pre-screening insurance questionnaires.

Marine insurance Act 1906

The insurance contract is regulated by the Marine Insurance Act 1906.[50] The Act regulates the contractual relationship between the insured and the marine insurers.[51] The insurer offers to assume risks in exchange for payments of premiums.[52] In establishing and understanding the marine insurance contract, section 1 of the Act should be read with section 3 of the Act. According, to section 1 of the Act, a contract of marine insurance is defined as 'a contract whereby the insurer undertakes to indemnify the assured, in the manner and to the extent thereby agreed, against marine losses, that is to say, the losses incident to marine adventure.'[53]

With regard to the United Kingdom's Marine Insurance Act 1906, although it does not apply to all marine insurance contracts. Section 3 of the Act provides that 'Every lawful adventure may be the subject of a contract of marine insurance.'[54] Furthermore, section 3(2) of the Marine Insurance Act 1906 defines Maritime Perils as 'the perils consequent on, or incidental to, the navigation of the sea, that is so say, perils of the sea, fire, war perils, pirates, rovers, thieves, captures, seizures, restraints, and detainments of the princes and peoples, jettisons, barratry, and other perils, either of the like kind or which may be designated by the policy.'[55] Marine insurance policies are subject to the Marine Insurance Act, failure to comply with the Marine Insurance provisions of the Marine Insurance Act may result in the contract being invalid.[56] Currently, the

[50] John Hare *Admiralty Jurisdiction in South Africa* 2nd edition (2009) at 838.
[51] Ibid.
[52] Ibid.
[53] Section 1 of the Marine Insurance Act 1906.
[54] Section 3 of the Marine Insurance Act 1906.
[55] Section 3(2) of the Marine Insurance Act 1906.
[56] Section 22, of the Marine Insurance Act 1906. 'Contract must be embodied in policy. Subject to the provisions of any statute, a contract of insurance is inadmissible in evidence unless it is embodied in a marine policy in accordance

contractual relationship between the cyber marine insurers and the insured is solely based on the principles of contract law and not regulated by the Act. The reason for this is that cyber risks are not recognized as marine perils or risks.[57]

with this Act. The policy may be executed and issued either at the time when the contract is concluded or afterwards.' F.D. Rose *Marine Insurance: Law and Practice* 2nd edition (2012) 155.

[57] Meixian Song *Causation in Insurance Contract Law* (2014) 86.

CHAPTER 3: CYBER RISK MANAGEMENT AND DAMAGE CONTROL

Introduction

As previously reiterated, Cyber risk is indeed a growing concern in the shipping industry. This applies not only to ship owners and port authorities, but also for marine insurers that have a mandate to provide reasonable covers that will reflect the risk in their premium, while remaining affordable.[58] This chapter will discuss possible ways that can be implemented to assess and manage cyber risks from the perspective of insurance companies.

As illustrated on the examples of chapter 2, there has recently been an increased occurrence of cyber-attacks, representing an extra risk that needs to be addressed.[59] With rate at which these cyber risks increase and spread, it is obvious that the related losses cannot be fully eliminated from materializing and therefore, emphasis should rather be placed on the manageability measures and its implementation respectively. There are several ways the insurers can manage their exposure; i.e. susceptibility to risk. The other way is to ensure the risks they cover are clearly defined and the amounts for which they are liable to indemnify the insured are controlled. The other is by requiring that the insured manages the levels of the risk to which it is exposed to by protecting itself against such (i.e. prevention).[60] Hand in hand with some of these preventive measures, such as e.g. two-factor authentication and conduct audits, the risk exposure can also be managed through the implementation of (and adherence to) the BIMCO and IMO guidelines, which will be described in more detail later in this chapter.

---

[58] Marsh 'Cyber Gap Insurance Cyber Risk: Filling the Coverage Gap' at 2, available at *www.oliverwyman.com/content/dam/marsh/Document/PDF/UKen/CyberGapInsuranceCyberRiskFillingtheCoverage,* accessed on 7 December 2019.

[59] World Maritime News 'In Depth: Cyberthreat Is Here to Stay!' available at *https://worldmaritimenews.com/archives/230822/interview-cyberthreat-is-here-to-stay/,* accessed on 1 December 2019.

[60] Ibid.

Cyber -risk assessment

It is undeniable that cyber risks are difficult to assess due to their hardly measurable impact and mainly lack of data, which are often kept secret as such revelation may not only further threaten the security of the attacked but also damage their reputation.[61] The cyber-crime techniques change rapidly and continuously making it complex for the insurers to keep up with the technologically progressive security measures that mirror the reactive savviness of the attackers. [62] Such dynamics and constant development of techniques and counter-measures troubles the insurers, making it hard for them to understand, quantify and assess the risks.[63] When combined with the implied 'hogging' of the valuable data, this process gets even more complicated in terms of its disputable transparency.[64]It therefore comes as no surprise that there is currently no scalable data model for insurers to assess and quantify such incidents.[65]

In order to overcome such hurdles, the author agrees with the publication by the SAFETY4SEA, which stipulates that the insurers need to have a clear understanding of the risk, while the insured should be compelled to have a contingency plan in place, in order to mitigate the likelihood of the extensive damage.[66]

The importance of such exercise is to narrow down the insurers scope of cyber risks assessment and guide them to deal directly with the challenge presented to them by the insured.[67] Simultaneously, the insurer should also instruct the insured to deploy adequate security measures in order to mitigate the risk exposure and, should this not be addressed, the insurer should not be liable for the damages or its full extent respectively.

---

[61] OECD 'Enhancing the Role of Insurance in Cyber Risk Management' (2017) at 111, available at *http://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf*, accessed on 15 December 2019.

[62] Ibid.

[63] Ibid at 124.

[64] SAFETY4SEA 'Cyber Security challenges for the shipping industry' available at *https://safety4sea.com/cm-cyber-security-challenges-for-the-shipping-industry/*, accessed on 07 September 2019.

[65] Christian Biener, Martin Eling and Jan Hendrik Wirfs 'Insurability of Cyber Risk: An Empirical Analysis' Geneva Papers on Risk and Insurance – Issue and Practice 40.1-28.10.1057/gpp.2014.19 at 17, available at *https://www.researchgate.net/publication/265727415_Insurability_of_Cyber_Risk_An_Empirical_Analysis/citation/download*, accessed on 04 January 2020.

[66] Ibid.

[67]Ibid.

According to study carried out by the European Insurance and Occupational Pensions Authority, there are several measures that the insurers can adopt to accurately quantify, evaluate and monitor the recorded patterns, while collecting the relevant data input related to cyber risk.[68] To achieve such optimization of the risk assessments and therefore also premium pricing (which will be discussed later), it is important, that the marine insurers engage with their intermediaries, actuaries as well as the policyholders, in order to gauge the risk while recording the details of the incident. In a long term, such input shall assist with the endeavor to achieve a reliable assessment of the threat likelihood, using the updated data in modeling, measuring and estimating of the impact on the business. Furthermore, such practice can also aid to determine the residual risk scores, top risks scenarios, control implementation and prioritized remediation guidance and expected loss range.[69] Additionally, establishing a robust assessment plan can also assist the insurer to identify whether the insurance market's preparedness is sufficient to assume cyber risks on behalf of the insured.[70]

Cyber risk management and the cyber risk guidelines in the marine industry

Cyber risk management can be defined as 'the process of identifying, analysing, assessing and communicating a cyber-related risk while accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders'.[71] Ships and ports operate within an internet dependent and digitalized environment, where operational risk management is inherently cyber risk management.[72] Currently, there are no cybersecurity

[68] European Insurance and Occupational Pensions Authority *Cyber risk for insurers-challenges and opportunities* what is this source? Is it a report? Is it an article? at 4, available at *https://eiopa.europa.eu/Publications/Reports/EIOPA_Cyber%20risk%20for%20insurers_Sept2019.pdf*, accessed on 1 December 2019.

[69] AIG '*Cyber Insurance: Executive Summary Report*'18 June 2018, available at *https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyber-executive-summary-report.pdf*, accessed on 5 December 2019.

[70] International Association of Insurance Supervisor 'Issues Paper on Cyber Risk to the Insurance Sector August 2016'at 25, available at *https://www.iaisweb.org/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector*, accessed on 10 December 2019.

[71] International Maritime 'Organisation Maritime Cyber Risk' available at *http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx* accessed on 10 December 2019.

[72] Gard 'Gard Alert: Managing cyber risks at sea' available at http://www.gard.no/web/updates/content/20912875/gard-alert-managing-cyber-risks-at-sea, accessed on 10 December 2019.

regulations in place to assists in managing cyber risks and likewise, the shipping industry has been very slow in implementing and publishing cybersecurity guidelines. Fortunately, following the 2017 cyber-attack on Maersk as previously described in the Chapter 2 of this dissertation, the IMO published Guidelines for the Cyber risk management. These guidelines are designed to help ship owners protect themselves from hackers, guiding the ship owners how to do so.

International Maritime Organization (IMO) guidelines

In 16 June 2017, the IMO Committee adopted a Resolution MSC. 428(98) titled Maritime Cyber Risk Management in Safety Management System (SMS).[73] 'The Resolution stated that an approved SMS should consider cyber risk management in accordance with the objectives and functional requirements of the ISM Code.'[74] Furthermore, on the 5th July 2017, the IMO issued MSC FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management.[75] Amongst the requirements listed within the above-mentioned directives, is the internal cyber risk management training for the shipowners employees whereby the owners and simultaneously policyholders (for the purpose of this thesis) are educated on the topic of cyber-crime.[76] The authority thereby attempts to ensure the adoption of the guidelines, as it gave ship owners and managers until 1 January 2021 to incorporate cyber risk management into their Safety Management System (SMS). To enforce that the measures are indeed implemented, the IMO stated that failure to comply will lead to risk of ships being detained by the port state control of the respective countries.[77]

[73] International Maritime Organisation MSC 98-23-Add.1 - Report of The Maritime Safety Committee on its Ninety-Eighth Session (Secretariat).pdf, available at *http://www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution%20MSC.428(98)%20-%20Maritime%20Cyber%20Risk%20Management%20in%20Safety%20Management%20Systems.pdf*, accessed on 02 December 2019.

[74] BIMCO 'The Guidelines on Cyber Security on Board, Version 3.0' at 13, available at http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16, accessed on 20 July 2019.

[75] International Maritime Organisation 'MSC-FAL.1-Circ.Guidelines on Maritime Cyber Risk Management (Secretariat). pdfhttp://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf*, accessed on 02* December 2019.

[76] Ibid.

[77] Gard 'It is time to strengthen your onboard cyber security procedures' available at *http://www.gard.no/web/updates/content/26742440/it-is-time-to-strengthen-your-onboard-cyber-security-procedures, accessed on 2 December 2019.*

Currently, the ship owners are still trying to meet the mentioned requirements despite the fact that the progress is very slow.[78] Therefore, it is important that the IMO and insuring institutions sustain the pressure put on the senior management of the shipping companies, and thereby remain actively involved to ensure that the guidelines are thoroughly implemented and exercised by the given date.[79] In order to avoid misinterpretation, it is important to emphasize that the recommendations as issued by IMO server primarily as a formal acknowledgement of the existence and severity of cybercrime in the shipping industry. However, it is quite essential to understand that the IMO guidelines alone are quite generic, rather serving as a mere reminder to incorporate security measures to manage cyber-crime. Therefore, it is of utter importance to recognize the references this publication makes to the best cyber security practices in the industry such as BIMCO guidelines and NIST framework, which are explained below. [17]

BIMCO -The Guidelines on Cyber Security Onboard Ship

In 2017, BIMCO together with other organizations (i.e. CLIA, ICS, INTERCARGO, InterManager, INTERTANKO, IUMI, OCIMF and WSC) published a version 1.0 of the Guidelines on Cyber Security onboard Ships focused on creating cyber awareness and risk management measures, that will aid the shipowners and operators to deal with the cyber incidents.[80] In 2019, the Version 3.0 was published, offering a guidance to shipowners and managers on how to develop the essential procedures and actions in order to improve cyber resilience, while maintaining integrity of systems onboard their ships.[81] The BIMCO Guideline is intended to provide assistance to shipowners and operators on how to assess their operation risks, identify the vulnerabilities in their systems and thereby take steps to protect themselves.

[78]International Maritime Organisational 'Interim Guidelines on Maritime Cyber Risk Management', *http://www.imo.org/en/MediaCentre/HotTopics/piracy/Documents/MSC1Circ1526%20%20Interim%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management.pdf*, accessed on 12 December 2019.

[79] BIMCO 'The Guidelines on Cyber Security on Board, Version 3.0' at 1, available at http://www.ics-*shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16*, accessed on 20 July 2019.

[80] INTERCARGO 'The Guidelines on Cyber Security onboard Ships' available at *https://www.intercargo.org/guidelines-cyber-security-onboard-ships/,* accessed on 20 December 2019.

[81] The Guideline on Cyber Security Onboard Ships V3 at 1, available at *https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=20,* accessed on 15 August 2019.

The Guidelines on Cyber Security Onboard Ships are aligned with the IMO's guidelines (specifically resolution MSC.428(98) and provide practical recommendations on maritime cyber risk management.[82] It is important to understand that the BIMCO guidelines are not a stand-alone document, as it is intended to be a complementary and supplementary set of exhortations to existing regulations under the International Safety Management Code (ISM Code) and the International Ship and Port Facilities Security Code (ISPS Code).[83] The Guidelines focus on six critical aspects of cyber security awareness namely: Identifying threats and understanding the cyber security threats to the ship; Identifying vulnerabilities within the ship's cyber security system; Assessing risk exposure and the likelihood of being exploited by external threats; Developing protection and detection measures in order to minimize impact; Establishing contingency plans to reduce the threat's impacts; and Responding appropriately to cyber security incidents.[84]

National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Another set of recommendations on how to enhance cybersecurity (and therefore also risk management), is the framework issued by the U.S. agency called National Institute of Standards and Technology (NIST). These general guidelines can be applied as yet another tool to manage and assess the cyber risks in marine industry and thereby help the policyholders to minimize the likelihood of successful cyber-attack.[85] These five elements are characterized by the following keywords: Identify, Protect, Detect, Respond and Recover.[86]

The "Identify" component directs the stakeholders to develop the organisational understanding of systems that, if disrupted, pose a serious threat, while aiding the risk assessment

[82]INTERCARGO 'The Guidelines on Cyber Security onboard Ships' available at *https://www.intercargo.org/guidelines-cyber-security-onboard-ships/,* accessed on 20 December 2019.

[83] The Guideline on Cyber Security Onboard Ships V3 at 1, available at *https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=20,* accessed on 15 August 2019.

[84]Ibid.

[85] Institute and Faculty of Actuaries *Cyber operational risk scenarios for insurance companies* (2018) at 8, available at *www.actuaries.org.uk*, accessed on 28 August 2019.

[86] National Institute of Standards and Technology (NIST) 'Cyber Security Framework' available at *https://www.nist.gov/cyberframework/framework,* accessed on 12 December 2019.

process.[87] Examples of such in the context of shipping industry may be the GPS infiltration due to importance of the system for the vessels navigation. In case of unauthorised access, the ships might end up in collision or spoofed, while being in the full control of the hackers. Hence, it is essential to have a master who is well aware of cyber- risks and trained on dealing with cyber-attacks on the navigation systems.

The second element, "Protect", aims to implement risk control management, processes and contingency measures, in order to ensure that in a case of cyber-attacks, the shipping operation does not get disrupted and can still continue.[88] The part three and four (i.e. Detect and Respond) of the framework focuses on the development as well as implementation of systems that can be used to detect the cyber incidents and adequately respond to them in a timely manner.[89] The last, quite self-explanatory component, i.e. "Recovery",[90] represents the measures put in place to help with a speedy recovery from the cyber-attack; e.g. back up of stolen data and/or regaining of the ship control.

It is critical that the above listed guidelines and measures are promoted by the insurer, persuading the policyholders to take all the necessary steps to safeguard against current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping. In return the insurer may offer incentives for the insureds that complies with these guidelines, e.g. discounts for implementing the guidelines. Not only will implantation of these guidelines be beneficial as a risk mitigator for the insurance companies, but they will also align with the interests of the policy holders to prevent their ships from being attacked and/or detained for non-compliance with the IMO guidelines as of 1 January 2021.[91]

As the aim, as well as some of the parts of this dissertation imply, it is essential that the insurance companies and shipowners work in synergy in order to achieve an optimal cyber risk exposure. The reason this dissertation proposes that the insurers enforce these cyber risks management elements to be implemented and complied with, is for the mutual benefit of lowering

[87] Ibid.
[88] Ibid.
[89] Ibid.
[90] Ibid.
[91] International Maritime Organisation' Maritime Cyber Risk' available at *http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx*, accessed on 2 December 2019

the likelihood of the attacks and thereby premium, as this fee is determined by the its frequency and the cost to compensate such risk. Thus, it is fair and reasonable that the insured be the one identifying e.g. easily targeted navigation systems, making sure that these are not easily accessible by the hackers, while also ensuring that the vessel is seaworthy before the commencement of the voyage. Furthermore, as a part of assessing the risks, the cyber marine insurer can use the 'Identify' component of NITS framework to assess the frequency of the occurrence of the cyber-attacks and severity of the cyber-risks.[92]

It is also useful to list other cyber-risks assessment measures that do not require any legal regulations and that can be implemented by the insurers in order to achieve a more exact premium pricing which will accurately reflect the reality. These include collection of past cyber data events, conduct of the interviews with affected parties including third parties and performance of qualitative risk assessment.[93] Part of assessing the risks involves establishing how the risks may affect the shipping and logistical operation and trying to come up with the best possible risk's assessment measures. Adhering to the NIST guidelines will assist the insured to identify the current and future risks and the extent of their impact on ships. Consequently, this shall also enable the insurer to create and measures that will reduce or circumvent the foreseeable risks.

Data security as a form of damage control

While some use the term risk management and risk prevention interchangeably, the author of this dissertation will refer to prevention as a 'tool' rather than management process discussed within the previous section. Currently, there is no standard method or modelling for the prevention of cyber risks.[94] Neither BIMCO nor the IMO has developed cybersecurity regulations that may be utilised to prevent cyber risks, as these guidelines rather focus on the holistic view of risk management.[95] Besides the mentioned, these current legal precedents in shipping do not cater for cyber loss and, as a result, prevention of cyber risk is very complicated.[96] Furthermore, it is

[92] Ibid.

[93] European Insurance and Occupational Pensions Authority 'Cyber risk for insurers-challenges and opportunities' at 8, available at *https://eiopa.europa.eu,* accessed on 01 December 2019.

[94] Ibid.

[95] Secure State Cyber Bog Post 'The Future of Maritime Cybersecurity' 15 April 15 2019, available at *https://securestatecyber.com/cyberbloggen-en/the-future-of-maritime-cybersecurity/*, accessed on 20 December 2019.

[96] Julian Clark 'The Changing Face of Maritime Law and Risk – Cyber, E-Commerce, Automation of Vessels': Maritime 2019' in *International Comparative Legal Guides 2019*, ICLG.COM 30 July 2019, available at

important that, at the moment, the cyber risk cannot be completely prevented from taking place and therefore, it is more accurate to refer to such 'preventive' efforts as a damage control or risk minimisation.

While the above-mentioned guidelines and frameworks target mostly the policyholders, while the insurers find themselves in a role of a 'supervisor' making sure that these are adhered to, this part distributes the liability for the damage more equally. Being the most active department that is trying to deal with cyber challenges, the cyber insurance market strives to fill in the gap of insufficient cyber related covers. Since the cyber risk problems result from technology, the most effective way to tackle those should be by implementation of cyber security.[97]

The dissertation previously touched on the topic of data leaks or data breaches, however, besides the part where the author discussed infiltration of navigational systems and the related leaks of e.g. ships location, this issue was not given enough attention from the insurers perspective, despite being often critical for the damage minimisation. It is important to realise that insurance companies store data that are related to e.g. cost of compensation in order to determine the premium. Likewise, these companies often dispose of details like cargo volume and available risk prevention measures, serving them to assess the risk. Should these leak – this will aid the cyber-attack perpetrator to target the right ship, i.e., to find the right ratio between the potential materialistic benefit and security elements that have to be bypassed.

Whether it is the insured policyholder or the insurance company itself, it is therefore utterly important that data security measures are implemented, in order to control the damage, which will once again result in a lower financial risk for the compensator (i.e. insurer) as well as increased affordability of the cover for the policyholder (i.e. shipowners).One of the solutions to data protection is undoubtedly the technology of blockchain, which works on the basis of decentralised data storage as oppose to conventional server storing. [98]

https://iclg.com/practice-areas/shipping-laws-and-regulations/2-the-changing-face-of-maritime-law-and-risk-cyber-e-commerce-automation-of-vessels, accessed on 9 September 2019.

[97] Ibid.

[98] KPMG 'Blockchain in insurance' available at https://home.kpmg/xx/en/home/insights/2018/09/blockchain-in-insurance-fs.html.'accessed on 03 December 2020. P Benchley 'How blockchain is tackling insurance industry challenges' at KPMG Insights *Blockchain in insurance* webpage, September 2018, available at *https://home.kpmg/xx/en/home/insights/2018/09/blockchain-in-insurance-fs.html*, accessed on 3 December 2020.

As a decentralised storage (often referred to as distributed ledger), this architecture operates within network which is based on so called consensus algorithm, where the distributed nodes need to agree on the validity of the access. As the name of this technological advancement suggests, the data are stored in blocks that are further linked into chain of those partitions. Therefore, blockchain will assist the insurers to protect their confidential information or prevent any unlawful adjustment, additional or deletion of their (the insurer's) data.[99] Unlike the classic and comparably more obsolete database architecture stored in a "client – server" settings and therefore more prone to data alteration by the third party using an unauthorized access, the blockchain offers an alternative securely scalable solution. It is therefore very likely that the implementation of blockchain would result in a significant decrease in data leaks in a short- terms and reduce the cost of cyber risk related losses in a long term.

Following the discussion related rather to physical security changes required to limit the damage for both – the insurer and the insured, it is important to remind the reader that in the context of this chapter, the prevention and damage control can be *de facto* understood as one. This is due to the fact that data security in a form of blockchain prevents the cyber-attack from taking place and, should it be attempted, minimizes the extend of the damage incurred. Should such concept be deployed during the incidents involving e.g. WannaCry and NoPetva viruses as described in Chapter 2, the financial damages would be far less costly, if any.

[99] Ibid.

CHAPTER 4: RISK CHALLENGES IN MARITIME TRANSPORT SECTOR

Introduction

As commonly emphasized in the previous chapters, the cyber risk represents a complex set of elements, which need to be addressed by insuring entities as well as their clients – i.e. policyholders. In terms of one of the oldest industries in the world – the shipping and ocean freight – this new phenomenon represents several challenges affecting both parties of the insurance market – i.e. the insurers and the insured. Unquestionably, cyber risk challenges are not only confronted by the shipping industry but other industries as well. The difference is the pace and manner in which these sectors deal with these risks. The shipping industry is slow in dealing and managing of cyber risks contrary to its increasing occurrence. It is common that before the insurer accepts to cover a certain risk there are several factors that they take into account. Such factors include the profile of the subject matter and the owner, the nature of the risk etc., as these are to determine whether such risk is insurable and if it is economically viable for the insurer. The following chapter lists some of the cyber risk challenges that are relevant to maritime industry, while having serious repercussions in regard to premium pricing. For better understanding, the author splits the challenges and their sources respectively between those faced by the insurers and those that are to be dealt with by the shipowners.

Challenges affecting insurers

As mentioned in the introductory part of this chapter, there is a number of cyber risk challenges confronted by the marine insurance companies. Nevertheless, for the purpose of this dissertation and in line with its aim, the author selected to only discuss several elements faced by the insurers due to their relevancy in terms of the influence on the premium pricing. Some of selected challenges include the following: cyber risk data collection inefficiencies, pricing and calculations of premiums, and risk of bankruptcy. As already implied in the previous parts of this paper, there is lack of reported cyber risk cases and therefore also deficiency of information and data related to these incidents which causes that some insurers refrain from covering cyber risk as this makes those events hardly quantifiable and rather unpredictable. Before elaborating further on the said issue, it is essential to introduce this challenge as one of the fundamental risks faced by the insurers

offering cyber risk cover for the maritime sector. Stemming from not having sufficient information on the historical cyber losses and damages, the insurance companies struggle in terms of the risk assessment, coverage extent and quantification of excess, which leads to limited coverage and high prices of premiums as these are based on critical assumptions instead of accuracy.

Lack of reported cases arises from the fact that the insured in most cases opt not to disclose their cyber-attacks ordeal in order to protect their business reputation.[100] Especially if the loss or damage is not of a major monetary value or the respective incident does not entail a loss of life and/or significant damage to the ship, the shipowners often refrain from reporting such event due to their impact on the brand of the company. Since there is no law that regulates cyber risks which, in this case, translates as no obligation for the insured to disclose any cyber incidents they experienced, it is believed to be a fairly common practice most likely taking place even more commonly should there be a financial participation on liability (i.e. excess) incurred[101]. Therefore, the insurance companies end up having difficulties in developing a data model due to missing records of the incidents.

As already mentioned, the consequence of unavailability of historic data are the inadequate insurance premiums and their calculation respectively, and as a result, the overpriced cyber risk covers. It is fair to say that currently, the cyber insurance coverage is more of an oligopolistic profit scheme, aiming at the financial benefits of the insurer rather than at closing of the cyber insurance gap.[102] However, despite the pricing being done by the insurers, it is also important to note, that these are subjected to information asymmetry, where the shipowners do not provide enough transparency in terms of the recorded attacks. This includes the completed cyber risk cases as well as the possibly attempted cyber-attacks, leaving the insurer in disadvantage in terms of information access, and therefore adding to ambiguity in terms of risk profiling. Such set up causes an imbalance illustrating how important is the collaboration between those two participating parties (i.e. insurer and the insured), when it comes to fairness in reporting and true reflection of reality in a form of premium pricing. It is clear that when reporting an attack or related incident, the

[100]Lloyd's List' Maritime industry must open up about cyber-crime' available at *https://lloydslist.maritimeintelligence.informa.com/LL1128745/Maritime-industry-must-open-up-about-cyber-crime,* accessed on 06 January 2020.

[101] Ibid.

[102] Ruperto P. Majuca, William Yurcik and Jay P. Kesan *The Evolution of Cyberinsurance Department of Economics: National Center for Supercomputinh Applications* (NCSA) at 2.

reputation of the carrier may suffer, however, without such there will be no data that would aid the insurance companies to tailor a reasonably priced cover. In order to change things around, the insurers may also try to manage these challenges by including incentive packages in their insurance policy, to encourage the affected policyholders to report the cyber-attacks they faced. Furthermore, such incentivisation could be further integrated with the already mentioned need to adopt (and comply with) cyber risks management guidelines i.e. IMO, BIMCO as well as NIST framework, as discussed in chapter 3. As a result, the insurer will have sufficient information that may be useful to calculate and price their premiums, while managing the risk. This will, in practice, lead to enabling the premium to be priced more accurately according to collected data, and its availability at lower cost due to increased risk management measures in place.

It is quite clear that on one hand there are no data to make a cyber risk a bit more predictable and thereby price the product in an affordable way. However, on the other, it is also the potential loss and its ambiguous extent that may simply represent too much risk for the insurers to take on. Should the insurer fail to specify the scope of the cyber-attack cover, it may likely result in significant financial loss or even bankruptcy. This, when combined with the unwillingness of the policyholders to pay higher premiums, creates the biggest challenge; i.e. establishment of the point where 'demand meets the supply', determining the market price. To reiterate this, we can use the argument echoed by the Lloyd's Chief Executive Officer (CEO) Inga Beale as she highlighted that 'In 2016, the stand-alone cyber market reached an estimated $3.5 billion in written premium, suggesting that this figure will double over the next two years.'[103] She further told the delegates at the Organisation for Economic Cooperation and Development (OECD) conference in Paris, that the issue of cyber insurance is still 'frustratingly immature, suggesting that the best way to address this ordeal is by establishing a partnerships.[104]

In the context of this thesis, partnership would imply a robust corporative relationship between the insured and the insurer such as e.g. insurance pooling. The analogy for emphasising on the establishment of a partnership being that it is undeniable that any insurance company that intent to assume cyber risks losses or the responsibility to indemnify the insured for cyber perils, is prone to run into a financial loss.

[103] Ibid.
[104] Ibid.

Therefore, establishing a partnership appears to be beneficial for both the insured and the insurer, as currently, the insurers have nothing concrete to base their premium calculations on. Hence their pricing is very high and, in some instances, exclusionary for medium and small shipping companies as they are unable to afford the monthly instalments.[105]

Challenges affecting policyholders

While the previous section dealt with the challenges faced by the insurers - primarily with the lack of data and the uncertainty of premium pricing derived therefrom, this part will put the discussed in the context of the insurers. Before we do so, it is essential to emphasize that some of the listed challenges are not isolated to impact one or the other subject of the insurance market, but rather both – insurers as well as insured. To put this in perspective, one of such issues that seems to show mutual repercussions is the mentioned premium pricing. While this issue represents a considerable amount of ambiguity and critical guessing for the insurer's perspective due to lack of data, the insured perceives this challenge in a form of overpriced cyber risk covers. Notably, it has been found that some policyholders are unable to afford cyber cover as the prices of the products are too high, while are simply unwilling to pay the price.[106] At the same time, some insurers argue that the reason they do not offer cover for cyber risks (or, if they do, charge exorbitant prices), is that the current entry price of premium that the insureds are willing to pay does not make a business sense for them due to potential of cyber perils and the related losses respectively.[107] Therefore, by charging high premiums the insurance companies are protecting their business as cyber losses can be extremely expensive and may, as already mentioned, lead to significant loses or even bankruptcy.

Another significant challenge faced by the shipowners (i.e. policyholders) are the qualifying expenses required to meet for the IMO guidelines compliance. Despite the published IMO Guidelines for the Installation of a Shipborne automatic Identification System (AIS) ordering

[105] Ibid.

[106] Staff Writer 'Cyber re/insurance market "frustratingly immature"': Inga Beale Lloyd's' in Reinsurance News 27 February 2018, available at *https://www.reinsurancene.ws/cyber-re-insurance-market-frustratingly-immature-inga-beale-lloyds/,* accessed on 9 December 2019.

[107] Naveen Goud 'Shipping companies are extremely vulnerable to Cyber Attack' Cyber Security Insider , at available at *https://www.cybersecurity-insiders.com/shipping-companies-are-extremely-vulnerable-to-cyber-attacks/*, accessed on 12 December 2019.

the ship-owners to have fitted AIS and install GPS navigation system, some ship-owners still operate their vessel on the old navigation system that is easily manipulated.[108]

Although these requirements were issued as long ago as the year 2000, some ship owners still find it difficult to have the AIS installed, as this sophisticated digital technology for navigation of the sea is quite expensive, especially for smaller business entities. Therefore, such small carriers often rather operate using old navigation system than to have updated navigation system, increasing the exposure to cyber risk due to increased cyber vulnerability. While the pricing of transition onto new navigation systems, as required by IMO, may represent a financial barrier for the shipowners, this also complicates the operations for the insurers as they have to be ones dealing with these two conflicting issues around old and new navigation system.

In this case, the insurer is more likely to charge the ship-owner that is not willing to comply the IMO guidelines; i.e. to have the AIS fitted, double the premium which is far from ideal as the stand-alone cyber product is expensive. Representing a reciprocal challenge, the insurance companies may, in turn, end up losing clients as the assured will then shop around for insurance cover that would suit their needs, likely excluding the cyber cover. Such choice may be further motivated by the existence of the Cyber Attack Exclusion Clause 380, which, in default, prevents the insurers from liability over cyber-attack, unless stipulated otherwise. [109] According to many the Cyber Attack Exclusion Clause 380 is the biggest contributor to cyber risk insurance gap as it excludes the cyber cover from some of the standard hull & machinery covers. In the past, there have been numerous attempts to remove or amend the exclusion of liability clause, however, with no luck, as some insurers are reluctant to make such change in order to protect their businesses. [110] Nevertheless, due to the increase in demand to have a cyber risk cover included, some of the hull and machinery insurers responded by offering cyber risk cover under a standalone-product at a higher premium. Additionally, it is also important to mention that International Group of Protection & Indemnity Clubs have always covered the cyber risks losses except of the ones that are politically or terrorism motivated.[111]

---

[108] Ibid.

[109] International Union of Marine Insurance Marine (IUMI) 'Marine cyber threat causing problem for t's & c's', *Insurance Marine News* 09 July 2019, available at *https://iumi.com/news/news/marine-cyber-threat-causing-problems-for-ts-cs*, accessed on 25 August 2019.

[110] Ibid.

[111] Institute Cyber Attack Exclusion Clause CL380:'1.1 Subject only to clause 1.2 below, in no case shall this insurance cover loss, damage, liability, or expense directly or indirectly caused by, or contributed to by, or arising

It is therefore clear that Cyber Attack Exclusion Clause 380 represents a significant challenge for the shipowners – especially in the combination with other mentioned barriers.
For the clarity reasons, it is certainly useful to quote an extract from the actual clause which reads as follows:'*...in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to 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 an electronic system*.'[112] As can be understood from the above, the most unfortunate part of this clause is that it does not respond to the existing trends of cyber risks' occurrence, as the liability over such is explicitly excluded.[113] Furthermore, the clause also excludes incidents such as loss of life, damage to property, oils spills and collisions – should these be inflicted, while linked to any computer related attacks. [114]
Partially related to the above is the next challenge; i.e. misunderstanding or lack of understanding of the cyber insurance covers. In some cases, the insured do not understand the terms and conditions of the cover they subscribe to, due to complexity of the system as illustrated on the exclusion clause. Hence, it is important, that at the pre-contractual stage, the insurer make the insured aware of the cover they will paying for; including any additions that may limit the scope of insurance.

Another substantial challenge faced by the shipowners is undoubtedly the limitation of claims of losses over the coverage cap, as some of the cyber-attacks damages may end up exceeding the selected cover.[115] The most difficult challenge faced by the insured in this regard,

---

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

[112] Tony Male 'Cyber Attacks Against Ships-Are you Covered?' available at *https://www.marsh.com/uk/insights-in-context/cyber-attacks-against-ships-htm,* accessed on 20 December 2019.

[113]EIOPA 'Cyber Risk for Insurers – Challenges and Opportunities' at 18, available at *https://eiopa.europa.eu/Publications/Reports/EIOPA_Cyber%20risk%20for%20insurers_Sept2019.pdf,* accessed on 08 November 2019.

[114] The Geneva Association 'Ten Key Questions on Cyber Risk and Cyber Risk Insurance' at 31, available at *https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-risk-10_key_questions.pdf*, accessed on 16 December 2019

[115] OECD 'Enhancing the Role of Insurance in Cyber Risk Management' (2017) at 72, available at *http://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf*, accessed on 15 December 2019.

is a demand for ransom by the cyber-attackers.[116]The hackers would normally use Malware to infiltrate the onshore systems or hack the navigation system, in order to gain control of the ship. Once they have gained full access of the vessel, they make a request for ransom, holding the members of the crew as well as the ship itself hostage. The liability for such damage (i.e., ransom payment), should the negotiations fail, is often unclear and therefore, the insurer may get re-insurances for cyber losses like this. From the perspective of the insured however, this can represent a significant challenge as the ransom demands are often high and the reinsurance for such liability non-existent. In extreme cases, such scenario may end up leaving the smaller shipowners with the only choice – paying the ransom and filing for bankruptcy.

Next challenge that has been regarded as one of the top ten risks of 2018, is the possibility of business interruption resulting from the cyber-attacks.[117] Self explanatorily indicating the extent to which can cyber-attack impact a shipping company, this scenario is feared by most of the shipowners. Therefore, it is advisable that the insureds don't underestimate the need to follow the risk management guidelines and damage control measures as discussed in chapter 3, in order to lower the risk exposure.

Last, but definitely not the least, is the challenge that was already acknowledged in the previous sections of the dissertation – i.e., damage of the shipowners' business reputation.[118] Reputational risk was considered as one of the top risks in 2019 ranking, as it came at number nine out of the ten most significant business risks.[119]

While some of the cyber risk losses are quantifiable and replaceable, the same cannot be said about loss of reputation as once it is lost, it may take ages to regain the trust and support from your old clients. In the meantime, the insured's business would be losing sales and thereby face the loss of

[116] Lloyd's List' Maritime industry must open up about cyber-crime' available at *https://lloydslist.maritimeintelligence.informa.com/LL1128745/Maritime-industry-must-open-up-about-cyber-crime,* accessed on 06 January 2020.

[117] Allianz Global Corporate & Specialty 'Allianz Risk Barometer 2019:Top Business Risks for 2019' at 4 available at *https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf*, accessed on 06 January 2020.

[118] Ibid.

[119] Allianz Global Corporate & Specialty 'Allianz Risk Barometer 2019:Top Business Risks for 2019' at 5 available at *https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf*, accessed on 06 January 2020.

revenue which may once again lead to the firm's liquidation.[120] Unfortunately for the insured, this is something that the insurer cannot be able to quantify or fix. Therefore, as previously mentioned, some of insured opt not to report their cyber incidents or cyber losses, in order to retain the status quo in terms of their business reputation.

One the challenges faced by the insurer is loss of cargo. Loss of cargo is regulated by Institute Cargo Clause. Loss of cargo should be treated the same as a loss covered by the Institute Cargo Clauses. Insured should be protection should any loss or damage be incited by hackers.

Challenges faced by the policymakers in Maritime industry: Contractual challenges

While some industries can be subjected to the blanket application of laws, marine insurance represents a specific field, where the application of the generic form of policies often appears unclear. The author is of a view, that in order to achieve a better understanding of the topic, it is useful to list some of these challenges faced by the policymakers. These scenarios include the treatment of collision of the ships caused by the cyber-attack, causation involving cybercrime and finally the principle of 'burden of proof' also referred to as the onus of proof.

Ship-collision liability

One of issues around cyber risk loss or claims is related to collision of ships. Collision is one of the perils of the sea that is recognised, what is not recognised, however, is when this incident happens due to cyber-attack. When negotiating the terms of the contract, the involved parties should clearly stipulate what must happen in case when the ship's navigation is hacked which, as a result, leads to collision or who is liable for collision that was caused by cyber-attack or spoofing. In this case the issue would be based on liability and onus of proof, which is also elaborated on within this section. As it is common that when one has suffered a loss before they can be indemnified for the loss suffered, they need to proof their clause and the cause and for a successful claim there must be a causal link between the loss and the damage.

[120] Munich Re 'Business interruptions due to cyber events: A challenging cover component' available at *https://www.munichre.com/topics-online/en/digitalisation/cyber/business-interruptions-due-to-cyber-events.html,* accessed on 06 January 2020.

Causation

The doctrine of causation is treated in depth in the law of delict.[121] As causation is one of the elements that must be met in order for one to have a successful delictual claim.[122] Causation is a factual inquiry and the test used is the 'But-for'[123] test also known as *conditio sine qua non* theory test. [124] Van der Merwe and Olivier explain 'but-for' test by stating that an act is the cause of a result if the act cannot be thought without the result disappearing simultaneously. The act must in other words be *conditio sine qua non* result, e.g. but- for the hacking the collision harm and damage incurred had the navigation system of the sea not being hacked the ship would have had a successful voyage. In this case the shipowner would argue hacking as the proximate cause of the loss.[125] However, but for the hacking the master lost control of the vessel and end up colliding with another ship. Collision is also treated fully under the law of delict for losses and damages suffered. Collision liability is also recognised as a peril of the sea and enjoys legal protection by the Marine Insurance Act.

The main issue here would the cause of action. The 'proximate cause 'of the loss of the perils of the sea i.e. collision. According to Neethling Potgieter, an academic legal writer for a successful claim there must be a causal nexus between the conduct and the damage.[126] The reason for this is that one i.e. the shipowner can be held liable for loss or damage that he has not caused. This is where the issues lie as in most cases the hackers are in a different jurisdiction with the ship. This might also raise fraudulent claims especially in a case of total loss as the insured may falsify their statement as state the reason for collision hacking, that before the ship ran aground the navigation system was hacked. That the hackers have gained full access control of vessel or offshore operations before the collision. For a successful claim a case of collision element of causation must exist and proved on a balance of probability.

[121] Neethling Portgieter *Visser Law of Delict* 7th edition (2014) at 183.
[122] Ibid.
[123] Ibid at 186.
[124] Ibid 185.
[125] Prof D. Rhidian Thoma *The Modern Law of Marine Insurance* at 35.
[126]Neethling Portgieter *Visser Law of Delict* op cit note 123 at 183.

Onus of proof

The general rule is that who alleges bears the onus of proof.[127] This principle is applicable in marine insurance and non- marine insurance claims safe to say in civil claims. The standard of proof is based on a balance of probability.[128] It is very low threshold compared to the criminal law cases. The plaintiff bears the onus of proof failure of which may lead to his or her claim being unsuccessful. The plaintiff is required to prove his loss. Applying the onus of proof principle this context collision as a peril of the sea, the shipowner will have to prove that indeed the vessel was seaworthy at the commencement of the voyage, that the master had adequate experience and qualification to sail the vessel and he attended cyber risk management training. That the ship was attacked, that the ship is insured, that the proximate cause of the collision was hacking. Furthermore, that had it not been the cyber-attack he would have incurred any losses and the ship would have not been involved in a collision. In addition, prove that the master did all he could to save the ship from collision as soon as he realised that the vessel's navigation system has been while on transit to complete a marine adventure. Based on the evidence presented by both the insurer and the insured the court will make ruling on which party is liable for the damages.

[127] Ibid at 250.
[128] Ibid.

CHAPTER 5: INSURERS' APPROACH TO CYBER RISK IN MARINE SECTOR

Introduction

The purpose of this chapter is to investigate the pre-contractual and contractual liability devices, as these are used by the insurer to rectify the risk levels. Such components and their terms respectively, should be considered by the insurance companies when deciding on whether to cover a risk and how to manage their exposure to liability. Currently, the contractual relationship between the marine insurers and the insured is solely based on the principles of contract law and not regulated by the Marine Insurance Act, nor recognised by the Standard Form Contracts and Clauses. The reason for this is that cyber risks are not recognised as marine perils or risks.[129] However, this does not the mean the cyber risk should be treated any different from any other risk.

The marine insurers' and shipowners' contracts are currently regulated by the common contract law, up until the stage where cyber risk is recognised as a marine peril. [130]Either way, the traditional tools incorporated or used by the non-marine and marine insurance are the same, when dealing with risk or pricing of premiums. Looking at the cyber-attacks holistically while taking into account various marine insurance contractual terms and the incidents covered (e.g., cargo losses, damage to the ship etc.), the author is of a view that such incidents should be recognised as a marine peril. This can be justified by the fact that the incidents take place on the sea and often target marine adventure insured by a voyage policy.

Pre-contractual stage

At the pre-contractual stage, both parties (i.e. the insurer and the insured) need to agree on the terms of contract. It is also important that the insureds cooperate with the insurers and provide them with any information that is privy to them. At the same time, this exchange gives both parties an opportunity to discuss and negotiate the terms of the contract and establish how the agreement can be beneficial for both parties. At the commencement of negotiations, it is necessary that the insured provide the insurer with all relevant details in relation to the insurable property failure

[129] Meixian Song *Causation in Insurance Contract Law* (2014) 86.
[130] Section 3(2) of the Marine Insurance Act 1906.

which will lead to the contract being valid or void. Depending on the severity of the conduct, the insurer will be able to cancel or rescind the contract. Below is the list of questions that the insurer should ask the assured at a pre-contractual stage. The duty to answer all the questions honestly is indispensable, as this will assist the insurer in assessing the risks. Following the breakdown of the pre-contractual questions, the author will elaborate on the two important principles that need to be applied i.e. the duty of disclosure and misrepresentation.

Pre-contractual insurance questions

a) What does the cyber risks coverage include?
b) Since cyber risk coverage is a standalone product by how much will the premium increase if I add cyber risk cover?
c) How much is the assured willing to pay on premium pay every month?
d) What is the scope of the cover and is the cover valued or unvalued?
e) What are the consequences of a breach of warranty?
f) Who is liable for damages or losses; whether is the shipper or the carrier?
g) What will happen in a case where the assured's insured subject matter is attacked, and the insured is unable to attach evidence to their claim form?
h) What will happen in a case of a total loss?
i) What will happen if the assured's ship still operates on an outdated navigation system of the sea? Will they still be covered and how will their premium be calculated?
j) How can the insured minimise and prevent their chances of being hacked?
k) How long does the parties have before the cancellation of the contract?
l) Is the insured allowed to have double insurance as a way of covering his loss or damages?
m) What if the employee is disgruntled, is he responsible for cyber risks?
n) What are the cyber risks assessment measures that put in place by the insured?

The above list includes examples of possible questions that prospective insurer considering offering cover against cyber-risks might ask. These are relevant in terms of the context and the aim of the dissertation as it is essential to understand the pre-contractual requirements that need to

be mutually discussed and understood before entering into agreement. The offered cover, its conditions and the price of the premium respectively, closely relates to how the potential client responds to these questions.

The duty of disclosure and fair presentation

At a pre-contractual stage, an insured has a duty to disclose all material information to the insure in order to reach the conclusion of the contract.[131] This could be anything from the number of times the ship has been attacked by hackers, the past damages and losses suffered at that point, the experience of the master, age of the ship, its voyage history as well as whether the vessel is fitted with the navigation system required by the IMO. Parallelly with the above, it is also important to stipulate whether the vessel in question is insured somewhere else. The reason for the above is to give underwriter data to assess whether they will be willing to cover the related risk exposure.[132]

Furthermore, in case where the insured decides to cover the risk, the information given will assist in pricing the premium and also aid the insurer when drafting their contract, setting the terms and conditions in which they are willing to cover the risks. For example, such draft may include answers to questions such as e.g. what is to happen in a case where the shipowner sails the ship with a crew that does not have cyber-attack training and ends up colliding with another vessel where the term of the contract requires the ship to be sailed by a master who went for cyber risk management training. It may also elaborate on the conditions under which the shipowner breaches a material term of the contract.

A duty to disclose information at a pre-contractual stage is very important, as failure to make a fair presentation could lead to the contract being cancelled. In terms of this principle, the insurers receive more information than the insured as they certainly need more protection due to existent information asymmetry. This is given by the fact that the vessels are in most cases in the hands of the shipowners who knows a lot about their history and have access to information that are unknown to the insurer. Supporting the above stated 'need for the fair distribution of relevant information', the shipowner, in most cases, knows the hot spot for cyber-attacks and the vulnerability of the navigation systems of their ships. As implied above, it cannot be expected for an insurance company to have knowledge of the previous attacks and vulnerability of the insured's

[131] Seminar Park *The Duty of Disclosure in Insurance Contract* (1996) at 8.
[132] Ibid.

vessel. This duty of disclosure and fair presentation was initially imposed on the insured by section 18 of the Marine Insurance Act 1906 before 12 August 2016 when the Insurance Act 2015 (c4) (UK)('Insurance Act 2015')[133] came into effect.[134] Also, it is essential to bear in mind that in instances where the Insurance contract does not deal thoroughly with the issue of disclosure, the Marine Insurance Act will apply. Subsequently, it is also prominent to emphasise that Insurance Act 2015 omitted the provisions of non-disclosure and misrepresentation. In this dissertation, the author first looks into principle of non-disclosure from the Marine Insurance Act 1906 perspective, before discussing it from the current law position. The doctrine of non-disclosure is embodied in the Marine Insurance Act in section 18.[135] The notion of disclosure plays an important role in all insurance and contract law.

Section 18 of the Marine Insurance Act imposes a duty on the insured to disclose any material information relevant to the contract at the pre-contractual stage that is privy to him or within his knowledge to the insured.[136] At the same time, the section 18 (1) entitles the insurer to avoid the policy where the assured omitted to disclose material facts to the insurer at the pre-contractual stage. Similarly, the Section 18(1) provides that 'The assured must disclose to the insurer, before the contract is concluded, every material circumstance which is known to the assured, and the assured is deemed to know every circumstance which, in the ordinary course of business, ought to be known by him. If the assured fails to make such disclose, the insurer may avoid the contract'.[137] Accordingly, the assured must disclose the material information that is privy to him before a contract of marine insurance is concluded.[138]

The principle of material information is emphasised in section 18(2) of the Marine insurance. Section 18(2) of the Marine Insurance Act provides that 'Every circumstance is material which would influence the judgment of a prudent insurer in fixing the premium, or determining

[133] Insurance Act 2015 (c4) (UK).

[134] Bryan Cave Leighton Paisner 'Insurance Act, innocent non-disclosure clauses and contracting out', available at *https://www.bclplaw.com/en-GB/thought-leadership/insurance-act-innocent-non-disclosure-clauses-and-contracting-out.html,* accessed on 24 November 2019.

[135] Section 18 of the Marine Insurance Act 1906.

[136] Ibid.

[137] Section 18(1) of the Marine Insurance Act 1906.

[138] Bilal Ahmad *The Pre-Contractual Duty of Good Faith- A Comparative Analysis in the Marine Insurance Contract Law with the Duty of Good Faith in the General Contract Law* (unpublished LLM thesis, Lund University, 2010) 25.

whether he will take the risk'.[139] The reason the duty of disclosure is placed heavily on the insured is because the insurer, when calculating or pricing the premium, relies on the information provided to him by the insured.[140] Thus, a failure to disclose material information during any negotiation stage of the insurance cover deprives the insured any opportunity to decide whether he is willing to insure the risks presented to him. As a result, in a case where the insured failed to disclose any relevant information a prudent the insurer would have to, the Marine Insurance Act entitles the insurer to repudiate the claim by raising a defence on non-disclosure.[141] It is important to emphasise that the insurer may seek the contract to be void even if even the assured's conduct of non-disclosure is an honest mistake, negligence or fraudulent as long the undisclosed information is material and ought to have been disclosed at the negotiations prior the conclusion of the contract.[142]

The difference between the Marine Insurance Act 1906 and the Insurance Act 2015 (c4) (U K) is within the issue of breach of a duty of disclosure. The Insurance Act provides that, where a duty of fair presentation is breached deliberately or recklessly, the insurer may avoid the contract, refuse all claims, and not return any of the premium paid. Despite working in synergy (i.e. none of the above Acts are repealed), the current law puts the insurer in a better position compared to the Act 1906 as in case of the latter, the insured may retain the premium. Insurer would, in this case, be in a better position in a sense that if the insureds are not honest or make a fair presentation, they can keep the premium.

For the purpose of this dissertation, the failure to disclose all material information and fair presentation to insurer by insured should be regarded as a very serious form of breach, especially considering the consequential financial losses arising from cyber-attack. In some instances, depending on the cyber loss or omission the insurer should be given an opportunity to deduct certain amount from the insured's premium before they return and cancel the insurance contract. Furthermore, in line with the aim of this dissertation, it is essential to understand how insurers and the insured are covered by the Marine insurance acts as these represent a significant risk mitigators, should the contract of insurance be breached. Therefore, such components and their deployment

[139] Section 18(2) of the Marine Insurance Act 1906.
[140] Ibid at 26.
[141] Section 18(1) of the Marine Insurance Act 1906.
[142] Section 18(1) of the Marine Insurance Act 1906.

should be reflected in the price of the premium, which, taken into consideration the 'Exclusion clause', will rise and fall in correlation with the cyber-risk exposure levels. Additionally, the premium price will also depend on how 'bullet-proof' the measures are implemented by regulators, as these represent an additional layer of risk management, predominantly from the perspective of the insurers.

The general contractual terms

A contractual term represents 'any provision forming part of a contract', where each term leads to contract obligation, which may, when breached, give a rise to litigation. [143]

In this part of the chapter, the author introduces the contractual tools that may be activated by the insurers, in order to protect their business interests, while mitigating and managing the risk through the regulation of liability. In line with the aim of this dissertation, this will serve to provide an understanding of the options that be adopted by the insurers in order to effectively deal with the peculiar challenges and uncertainty imposed by the cyber risks, while once again aiming to activate these in the favour of lower risk and therefore decreased cost of premium. As stipulated earlier, the high prices of the premiums and the Exclusion clause appear to be the main contributors towards the existent insurance gap.

Indemnity

The principle of indemnity is dealt with in the sections 67-78 of the Marine Insurance Act 1906.[144] Indemnity is a fundamental term of insurance contract and the insurer may indemnify the insured for the insurable property that is agreed upon.[145] The Marine Insurance Act makes this a clear in the definition of insurable interest as it highlights that there must be a physical object exposed to marine perils.[146] Furthermore, it also stipulates that the insured must have some legal relationship

[143] E.Martin *Oxford Dictionary of Law* 6th ed (2006), available at https://www.oxfordreference.com/view/10.1093/acref/9780199551248.001.0001/acref-9780199551248, accessed on 12 January 2020.

[144] Section 67-78 of the Marine Insurance Act 1906.

[145] John Hare op cit note 52 at 857.

[146] Ibid.

to the object, in consequence of which, he benefits by its preservation and is prejudiced by loss or damage happening to it, or, where he may incur liability in respect thereof.[147]

However, the absence of an 'insurable interest'[148] in the subject matter at the time of the conclusion of a contract, does not invalidate the contract, as the agreement can only be invalid only if the insured is found to have been 'gambling'.[149] If the insured has an expectation of acquiring an insurable interest after the contract has been concluded, then it is unlikely that it would be found to have been gambling by concluding the contract. It is important to note. That the absence of an insurable interest at the time the of the conclusion of the contract, does not render the contract void. It simply means that the insured has suffered no financial loss and therefore the insurer has no obligation to indemnify the insured. Additionally, the insured is not obliged to have an insurable property at the time of concluding the contract as long as he intends to have that property or shows that he intends to have an insurable property and that he is interested in a marine adventure.[150]

What is more important is that at the time of the claim, the insured must have such insurable property in order to have a successful claim.[151] In the context of this dissertation, the shipowners are required to at least have an interest in a marine adventure, if at the time of concluding the contract, he did not have an insurable property. However, as already highlighted, at the time of a claim, such an insurable interest must exist. Lastly, no insurable property e.g. a vessel, cargo etc. implies that the insured has suffered no loss and therefore, there is no need to indemnify him. The main objective of the insurance is to indemnify or reimburse the insured for the loss suffered in exchange for the insured paying an agreed premium amount in order to put the

[147] Section 5 of the Marine Insurance Act 1906.

[148] Ibid.

[149] Section 4 of the Marine Insurance Act 1906. 'Avoidance of wagering or gaming contracts(1) Every contract of marine insurance by way of gaming or wagering is void.(2) A contract of marine insurance is deemed to be a gaming or wagering contract--(a) Where the assured has not an insurable interest as defined by this Act, and the contract is entered into with no expectation of acquiring such an interest; or (b) Where the policy is made 'interest or no interest,' or 'without further proof of interest than the policy itself.' or 'without benefit of salvage to the insurer,' or subject to any other like term: Provided that, where there is no possibility of salvage, a policy may be effected without benefit of salvage to the insurer.'

[150] Section 5 of the Marine Insurance Act.' Insurable interest defined (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.'

[151] Ibid.

policyholder in the financial position they were before they suffered loss.[152] Depending on the loss, the insured may be indemnified in a form of replacing the property or in a monetary term.[153] Since cyber losses are quite extensive, it would be advisable for the insurer to cover the cyber risk under a 'valued policy'.[154] Since the cyber losses are always costly, it would be economically sensible for the insurer to offer cyber risk cover or indemnify the insured on a valued policy. A valued policy or fixed policy can be used a tool to limit their losses.'[155] In a case of cyber-attack, the proximate cause for loss of cargo or demurrage claim would be a hacked navigation of the sea system. Because, had it not been the hacking of the navigation system, the master would not have to face any offshore challenges e.g. loss of cargo as there would not be any spoofing or delay of cargos nor stolen cargos. One of the tools that the insurer can use to limit their liability is the mutual consensus; i.e. the insured and the insurer to agree on the sum insured.[156] Basically, in this case, the amount of money the marine insurer is willing to pay for the cover. This will assist in terms of avoiding any confusion when loss or damage has been incurred.

Excess

Insurance excess can be understood as the amount paid by the insured when making a claim, prior to any action taken by the insurer to fix or replace the subject matter. Excess may only be paid after an insured has suffered a loss.[157] Excesses can also be used as a tool that prevent the insured from claiming for small damages or making frequent claims.[158] It is also important to note, that an amount set for excess differs from one insured to another, depending on the premium paid by the insured. If the insured's premium is high there is a likelihood that insured will pay less on their excess and vice versa.[159] In the shipping industry, the insureds are already complaining about the high premium. Therefore, in a case like this (even though risks are high), the insurers should try

[152] Ibid at 9.

[153] Ibid at 8.

[154] Section 27 of the Marine Insurance Act 1906.Valued policy. 27.—'(1) A policy may be either valued or unvalued. (2) A valued policy is a policy which specifies the agreed value of the subject-matter insured.(3) Subject to the provisions of this Act, and in the absence of fraud, the value fixed by the policy is, as between the insurer and assured, conclusive of the insurable value of the subject intended to be insured, whether the loss be total or partial.(4) Unless the policy otherwise provides, the value fixed by the policy is not conclusive for the purpose of determining whether there has been a constructive total loss.'

[155] MFB Reinecke, JP van Niekerk & PM Nienaber *South African Insurance Law* (2013) at 8.

[156] Ibid.

[157] John Hare op cit note 52 at 859.

[158] Ibid.

[159] Ibid.

to establish a balance, making sure that at least the insured pay a small amount for excess when they make claims.

Warranty

Another noteworthy term that is used by insurers to approach cyber risk, is warranty. It is always important and advisable to insert a warranty clause in the insurance policy. As this assist in terms of limiting losses and damages claims. In some instances where there is a breach it might assist insurer to escape liability. A warranty is considered as an undertaking or a strict insurance term in an insurance contract.[160] A warranty is regulated by sections 33 - 41 of the Marine Insurance Act and is defined as a 'condition on which the contract is founded'.[161] In terms of sections 33 (1) a '*warranty, 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.*'[162]

A warranty is a condition precedent that impose a duty of compliance on the insured.[163] Furthermore, according to section 33(3) there are two types of warranties the implied or expressed warranties.[164] For the purpose of this dissertation the focus will be on the implied terms so to say seaworthiness. A breach of a warranty from an English Law position has a precarious legal effect, an insurer is discharged from liability from the date of breach.[165] The English Law does not require an insurer to make an election to cancel the contract, the insured's non-compliance of a material term in the policy is sufficient. This principle was subsequently employed in Bank of *Nova Scotia v Hellenic Mutual War Risks Association (Bermuda) Ltd, 'The Good Luck'*[166] this case before Lord Goff was concerned with a breach of warranty in a marine insurance. Lord Goff made clear that a breach of warranty automatically discharges the insurer from liability from the day of breach.[167] However, this provision from the current law has omitted words such 'as from the date of breach

[160] MFB Reinecke *et al* op cit not 157 at 295.
[161] Sections 33-41 of the Marine Insurance Act 1906.
[162] Section 33(1) of the Marine Insurance Act.
[163] John Lowry, Philip Rawlings & Robert *Insurance Law: Doctrines and Principles* op cit note 143 at 217.
[164] Section 33(1) of the Marine Insurance Act.
[165] Section 33(3) of the Marine Insurance Act.
[166] *Nova Scotia v Hellenic Mutual War Risks Association (Bermuda) Ltd, 'The Good Luck'* [1992] 1 AC 233.
[167] Supra at 202.

of warranty'.[168] The insurer is still discharged from liability, however, not from the date of breach of warranty. There are two types of warranties; the implied and expressed warranties. For the purpose of this dissertation the implied warranty precisely unseaworthiness of ship will be discussed. The doctrine of seaworthiness of the ship is regulated by Section 39 of the Marine Insurance Act.[169] Section 39 (1) highlights that the ship's seaworthiness is evaluated at the commencement of the voyage or marine adventure,[170] Section 39 (2) establishes that the ship is considered to be seaworthy if it can' reasonably fit to encounter the ordinary perils of the port'[171] and section 39(4) support this by stating that the vessel is considered to be seaworthy if it has the ability to maneuverer through the necessarily expected or ordinary perils of the sea.[172] In *McFadden v Blue Star Line*,[173] Channel J held that for a vessel to be considered seaworthy it 'must have that degree of fitness which an ordinary, careful and prudent owner would require his vessel to have at the commencement of her voyage, having regard to all the probable circumstances of it'.[174] Furthermore, 'A ship is deemed to be seaworthy if she is in a reasonably fit state as to repairs, equipment, crew and all other respects to encounter the ordinary perils of the voyage insured'[175] at the commencement of the voyage. Conversely, looking at these definitions of seaworthiness it clear that a vessel is deemed to be seaworthy if it has the ability to encounter 'ordinary perils'[176] of the sea and of the port at the commencement of the voyage.[177] However, it does not mean that the ship will not be considered to be seaworthy simply because it failed to complete the shipment. As long as the commencement of the voyage when assessed the ship is deemed to be fit to encounter the ordinary perils of the sea. [178]

In a case of cyber risk, it is important that the insurer incorporate a warranty clause in their policy to protect themselves from unwarranted losses and also the insured. This can be achieved

[168] Section 10(7) of the Insurance Act 2015 (c4) (UK).
[169] Section 39 of the Marine Insurance Act 1906.
[170] Section 39(1) of the Marine Insurance Act 1906.
[171] Section 39(2) of the Marine Insurance Act 1906.
[172] Section 39(4) of the Marine Insurance Act 1906.
[173] *McFadden v Blue Star Line* [1905] 1 KB 697.
[174] Supra at 671.
[175] *Moir v Royal Exchange Ass Co* (1815) 4 Camp 84.
[176] F.D. *Rose Marine Insurance Law and Practice* at 200.
[177] Baris Soyer *Warranties in Marine Insurance* 3rd edition (2017) 63.
[178] F.D. Rose op cit note 178 at 200.

by imposing a duty on the insured to adopt the IMO Guidelines for the installation of a shipborne automatic identification system (AIS). This is for the purpose of ensuring that vessel is seaworthy that the vessel is seaworthy at the commence of the voyage and that the hackers cannot easily hack ghost the vessel. Since the IMO Guidelines for the installation of a shipborne automatic identification system (AIS)' requires ships to be fitted with AIS and GPS for navigation of the sea, any vessel that is not equipped with the required digital navigation system is deemed unseaworthy and considered as not going to be able to overcome any ordinary perils of the sea i.e. cyber-attacks. Thus, in a situation where a vessel was spoofed as a result, the insurer would be automatically discharged from liability. The insurer's defence would be that the insured breached a warranty that is material to the risk or the contract. As a result, of non-compliance of such condition precedent the insured sustained loss and damages that could have been avoided. Furthermore, it is important to note that the principle of seaworthiness is not limited to AIS it can also be extended to the master who is unable to operate or unskilled to use these advanced digital n avigation systems.

CHAPTER 6: COMPARISON OF CYBER RISK POLICIES

Introduction

Currently the cyber risks are fully covered by the International Group of Protection & Indemnity Clubs. Like hull and machinery, the P& I Clubs have their own exclusion of liability clause. The reason for this is to limit their scope of liability. Since the outcry and demand for cyber risk cover some hull and machinery and some non-marine insurance have joined the force to offer cyber-attack cover to shipowners. This includes Lloyds, AIG, Beazley Cyber Defence for Marine and Allianz Global Corporate & Specialty. For the purpose of this dissertation, the following P&I Clubs and insurance companies' policies will be examined and compared: Swedish Club; North P & I; Gard; Steamship Mutual; The American Club; Britannia P&I; Standard Club; Ship Owners Club; Japan Club; NEPIA; AIG; Lloyds and Allianz Global Corporate & Specialty. The reason for this comparison is to choose the most suitable policy that can potentially aid to close the gap in cyber insurance for ship.

P &I Clubs and other cyber risks insurance cover policies

The Protection & Indemnity (P&I) insurance covers is limited to risk agreed upon in their policy and subject to the Marine Insurance Act. P & I Club insurance covers shipowners for specific or only 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. Below are the different types of P&I Clubs and the extent of their policies.

North P & I Club

North P & I Club is one of the Clubs that does not cover cyber risks. Its policy incorporates the Institute Cyber Attack Exclusion Clause CL 380.[179] Still, similarly other clubs, the North P&I Club excludes the losses and damages from the computer virus and war and terrorism cyber- attacks.[180] The North P&I Club furthermore, excludes the losses caused by computer virus.

[179] North Club *P&I Rules (2019-20)* at 46, available at *https://www.nepia.com/latest/all-publications/rule-books-and-recommended-clauses/,* accessed on 02 December 2019.– accessed 12 January 2019.
[180] Ibid.

Standard Club

Standard Club covers cyber risks, what is excluded is paperless trading and incorporation The club covers cyber risks if the loss does not arise from terrorism or another war risk.[181] However, if harm was inflicted or perpetrated by an individual or group for the purposes of causing general disruption and for no public cause, then this would be very unlikely to constitute terrorism and therefore excluded in the cover.[182] Furthermore, if a cyber-attack was 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.[183]

Gard P& I Club

Gard does not incorporate the Institute Cyber Attack Exclusion Clause CL 380. [184] According to Gard Rules 2019, the Club is not liable for any losses, liabilities, costs or expenses directly or indirectly caused by, contributed to, or arising from harm of any computer virus.[185] Furthermore, Clause 4 of the Rules provides that Guard shall not cover to losses arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.[186] It is clear from the Rules that cyber risk losses are covered as long is not war or terrorism incited.

Japan P&I Clubs

The Japan P& I Japan P&I Club's policy cover cyber-risks is broken down into to external factors and internal factors. External factors are explained as unauthorized access, system hacking, viruses, social engineering and the internal factors as operational mistakes and includes general

[181] Standard Club 'P&I Club and Defence Correspondence Rules 2019/20' at 66, available at *https://www.standard-club.com/media/2768106/pi-and-defence-rules-and-correspondents-2019.pdf,* accessed on 06 January 2020.
[182] Ibid.
[183] Rupert Bank 'Cyber Risk & P& I Insurance Implication' at 2, available at *https://www.standard-club.com/media/2533617/cyber-risks-and-pi-insurance-implications.pdf*, accessed on 01 December 2019..
[184] Gard 'Rule 2019' at 102, available at *http://www.gard.no/Content/27095618/Rules_2019_web.pdf, accessed on* 02 December 2019.
[185] Ibid.
[186] Gard 'Gard Rules, 2019' at 102, available at *http://www.gard.no/Content/27095618/Rules_2019_web.pdf,* accessed on 01 December 2019.

system failures.[187] Japan P&I Club does not offer cover for any cyber risks inflicted by a computer virus.

Britannia P&I

According to the Britannia Protection & Indemnity Rules and Correspondence Class 3/2019/20, it is clear, when examining the exclusion of liability clauses and Paper Trading clause, that there is no cyber-risk exclusion or even computer virus exclusion.[188] The Club /Association does not incorporate Institute Cyber Attack Exclusion Clause – Cl. 380.

Shipowner Club

Shipowners Club does not cover Chemical, Bio-chemical, Electromagnetic Weapons Exclusion Clause, while incorporating the exclusions of liability clause.[189] The Club's Rules expressly exclude computer virus coverage loss or damage.[190] Furthermore, the Club excludes liabilities, costs and expenses caused by usage of electronic paperless trading systems.

AIG

AIG is one of the general insurance companies that offers cyber insurance cover for ships.[191] AIG assists insureds to understand and address cyber risk better, with comprehensive services, support, while taking into consideration their business and protective interests.[192] So far, the AIG cyber risk policy may be graded as the best cyber insurance policy.

AIG policy also provides for bodily injury, property damage, business interruption and product liability and likewise includes third party damage to property and third part injury, as well as cyber

[187] Cyber risk and Cyber Security Countermeasures. (2018). 'Japan P&I Club Loss Prevention Bulletin,' available at *https://www.piclub.or.jp/wp-content/uploads/2018/05/Loss-Prevention-Bulletin-Vol.42-Full.pdf,* accessed 06 January 2020.

[188] Britannia P&I 'Britannia Streaming Protection & Indemnity Rules and Correspondence Class 3/2019/20' at 49, available at *https://britanniapandi.com/rule-books-for-2019-20-policy-year/*, accessed on 06 January 2020.

[189]The Shipowners' Club '*Club Rules 2019* at 117, available at *https://www.shipownersclub.com/media/2019/02/Club_Rules_2019_Web.pdf*, accessed on 20 November 2019.

[190] Ibid at 42.

[191] AIG 'Cyber Liability', available at *https://www.aig.co.za/business/products-services/financial-lines/cyber,* accessed on 20 November 2019.

[192] AIG 'CyberEdge® Plus Cyber-attack related bodily injury, property damage, business interruption, and product liability', available at *https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-plus.pdf*, accessed on 20 November 2019.

extortion and data breach. [193] Like any other cyber risk insurance, the AIG offers cyber risk cover as a standalone cover.

Additionally, the AIG's insurance policy is divided into the following types:

- CyberEdge covering the financial costs linked to the breach, first party costs including event management, data restoration, third parties' financial loss, business interruption and cyber extortion.[194]
- CyberEdge® Plus which covers physical losses and damages caused by cyber-attacks, business interruption, first- and third-party property's objective is to protect the interest and property of the insured, it delivers express excess coverage for bodily injury, property damage, and financial loss resulting from a cybersecurity failure.[195]

The cover is, however, also subjected to AIG's Exclusion of Liability Clause, which stipulates that the insurer shall not be liable to make any payment for loss that is:

'(a) arising out of, based upon or attributable to any dishonest, fraudulent, criminal or malicious act, error or omission, or any intentional or knowing violation of the law, if committed by any: (1) past or present director, officer, trustee, general or managing partner or principal (or the equivalent positions) of a Company, whether acting alone or in collusion with other persons; or (2) past or present employee (other than those referenced in Sub-paragraph (1) above) or independent contractor employed by a Company if any person referenced in Sub-paragraph (1) above participated in, approved of, acquiesced to, or knew or had reason to know prior to the act of, the dishonest, fraudulent, malicious, or criminal act committed by such employee or independent contractor that caused a direct loss to an Insured or any other person. (b) arising out of, based upon or attributable to any misappropriation of an Insured's trade secret, any misappropriation of a trade secret by an Insured or any employee of an Insured or any infringement of patent, copyright, trademark or trade dress. (c) arising out of, based upon or attributable to any (1) presence of Pollutants; (2) the actual or threatened discharge, dispersal, release or escape of Pollutants; or (3) direction or request to test for, monitor, clean up, remove, contain, treat, detoxify or neutralize pollutants, or in any way respond to or assess the effects of

[193] AIG 'Cyber Coverages: Four Steps to Prepare for and Defend Against an Imminent Cyber Attack' available at *https://www.aig.com/business/insurance/cyber-insurance*, accessed on 10 December 2019.

[194] AIG 'Cyber Insurance' available at *https://www.aig.com/business/insurance/cyber-insurance,* accessed on 10 December 2019.

[195] Ibid.

Pollutants. (d) for any Bodily Injury or Property Damage. (e) arising out of, based upon or attributable to any: (1) fire, smoke, explosion, lightning, wind, water, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, act of God or any other physical event, however caused; (2) war, invasion, military action (whether war is declared or not), civil war, mutiny, popular or military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against any of these events; or (3) satellite failure. (f) arising out of, based upon or attributable to any seizure, confiscation, nationalization, or destruction of a Computer System or Electronic Data by order of any governmental or public authority. (g) arising out of, based upon or attributable to any Security Failure or Privacy Event, or any Related Acts thereto, which has been reported, or in any circumstances of which notice has been given, under any policy of which this Event Management Coverage Section is a renewal or replacement or which it may succeed in time. (h) for any profit or advantage to which any Insured is not legally entitled. (i) arising out of, based upon or attributable to any amounts for: (i) the original creation of; (ii) diminution of value of; (iii) lost profits of; (iv) or loss of use of, a trade secret, patent, copyright, trademark, trade dress or any other intellectual property.'[196]

The AIG cyber marine insurance cover appears to be one of the well drafted policy as it contributes significantly to the idea of closing the insurance gap. The AIG policy reflects the interest of both parties and appears quite comprehensive, compared to other policies.

However, the cyber cover might have a high premium since is a stand- alone product, but at least, all the covers are broken down in a way that is serves the interests of each insured. Furthermore, the AIG offers a cyber insurance that is more than just a compensation for potentially significant financial losses as it includes their advice on prevention and ways to respond to incident. This cover also constitutes of tips to improve the shipowners' cyber resilience and suggests mitigating measures through their 24/7 customer care.[197]

[196] AIG 'Liability Protect Policy Tour' available at *https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Liabilities/liability-protect-policy-tour.pdf*, accessed on 20 November 2019.

[197] AIG 'CyberEdge® Plus Cyber-attack related bodily injury, property damage, business interruption, and product liability' available at *https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-plus.pdf*, accessed on 20 November 2019.

Allianz Global Corporate & Specialty (AGCS)

Allianz Global Corporate & Specialty (AGCS) is one of the insurance companies that has offered cyber insurance for years.[198] It has been offering cyber insurance on 'stand-alone' basis, incorporating the traditional property and casualty policies.[199] AGCS just like AIG offers first-party and third-party losses. The first-party losses include a business interruption, restoration, and crisis communications while the third-party losses cover data breaches, network interruption, and notification expenses.[200] However, similarly to AIG, the AGCS cyber insurance offers much more than just compensation for potentially significant financial losses.

Lloyd's

Lloyd's cyber risk policy covers a physical loss from cyber risk, indemnifies third-party for physical damage and business interruption loss and, in addition, offers a cover for crisis management, IT forensics, cyber extortion, digital asset restoration and privacy liability.[201]

However, it is not clear whether the additional support, such as assisting the insured in a case of cyber incident crime management will be favored by the policyholders, especially if it means additional money on top of the stand-alone product. Examples of this include but are not limited to: credit, political risk, contract frustration, financial guarantee insurance, surety bond reinsurance, contingent business interruption, event cancellation and specialist contingency covers, construction delay-in-start-up, travel, directors' and officers', commercial crime insurance, errors and omissions and other specialist professional indemnity products.[202] Lloyd's offers insurance for perils arising as a consequence of terrorism reinsurance, political violence, cyber-attack, health insurance, workers' compensation and other commercial casualty covers, kidnap and ransom, contingency products, travel insurance, business interruption and contingent business interruption.

[198] Allianz Global Corporate & Specialty 'Cyber Insurance' available at *https://www.agcs.allianz.com/solutions/financial-lines-insurance/cyber-insurance.html,* accessed on 01 December 2019.

[199] Ibid.

[200] Ibid.

[201] Lloyd's 'Lloyds City Risk Index' available at *https://cityriskindex.lloyds.com/about/*, accessed on 06 January 2020.

[202] Ibid.

Lloyd's cyber insurance policy aims to protect the insured's business and responds to the growing challenges of cyber risk faced by their clients. Since Lloyds are aware that cyber data breach has serious implications on the operations and reputation of the insured, the company offer assistance in a form of consultation with cyber expert on ways to improve their security and mitigate the risks.[203] Lloyd's Data Breach Response Policy goes beyond the standard cyber risks insurance cover as it also offers a service which helps insured manage the aftershock of a breach as well as providing cyber insurance cover for the costs of notifying clients, forensic investigations, credit monitoring for customers, legal costs and public relations services to help manage any reputational harm.[204]Lloyd's policy offers cover for third party claims and associated defence costs arising out of a data breach; coverage for the defence costs associated with regulatory investigations; for ransom demands and malicious threats; costs in relation to restoring the organisation's affected systems; coverage for the income loss resulting out of interruption and assistance in restoring the data, network and IT system.[205]

Beazley Cyber Defence for Marine

In May 2019 Beazley introduced a new cyber insurance policy called Beazley Cyber Defence for Marine designed to cover physical damage and loss of hire.[206] It is also a form of a standalone cyber insurance. Beazley Policy is more accommodative and effective compared to some P&I Clubs cover. Beazley's marine cyber insurance cover is divided into two forms.[207] The first cover provides for operational technology policy. The policy covers physical damage on ships and responds in the event of cyber incident. In addition, assist the insured understand cyber risks assessment and ways on preventing and cyber risks mitigation.[208] The insured in a case of financial

[203] Lloyd's 'Cyber products at Lloyd's' available at *https://www.lloyds.com/about-lloyds/what-lloyds-insures/cyber/cyber-products,* accessed on 12 December 2019.
[204] Ibid.
[205] Lloyd's 'Why buy cyber insurance at Lloyd's? available at *https://www.lloyds.com/about-lloyds/what-lloyds-insures/cyber/why-cyber-insurance*, accessed on 12 December 2019.
[206] Beazley Cyber Defence for Marine Comprehensive loss of hire and physical damage cyber protection for single commercial vessels and fleets' available at *https://www.beazley.com/documents/Factsheets/beazley-cyber-marine-brochure.pdf*, accessed on 20 July 2019.
[207] Ibid.
[208] Ibid.

loss of hire he can claim up to US$5 million and up to US$50 million for physical damage.ie. property loss.[209]

Second policy provides for data and information technology protection. This cover cyber risks causing business interruption, cyber extortion data recovery costs, data network loss and eCrime.[210] In addition, Beazley marine insurance policy offers cover for legal services, computer forensic services and provides accessible 24/7 call center services for their clients in cases of cyber risks threats. Furthermore, provides a credit monitoring, identity monitoring or other personal fraud or loss prevention solutions, public relations and crisis management expenses.[211]

Arising from this exercise, the one common thing they have is that no P&I Club covers liability arising from war and terrorism. It is also to important highlight that the P& I Clubs exclude coverage for property damage, loss of life, third party liability, business interruption cargo loss and pollution resulting from data breach.

[209] Ibid.
[210] Ibid.
[211] Ibid

CHAPTER 7: CONCLUSION

For decades, the shipping industry has been known for being conservative and traditional. Despite this, it is now forced to evolve and address the cyber related risks, as these became a serious threat with the field's growing dependency on technology.

This dissertation was set out to investigate how the insurers and their clients deal with the challenges arising from such modernization and how could an appropriate and affordable insurance cover be facilitated, in order to operate to satisfaction of both parties, while covering the identified insurance gap. Simultaneously, the author puts an emphasis on the importance of investigation, recording and management of the offshore cyber risks incidents and compares the available insurance products to determine the best source of inspiration for the future enhancements. Although, the marine authorities introduced cyber risk management guidelines aimed at creating cyber risk awareness and cyber risk management, shipowners still seem to face the increasing trend of cybercrime due to rapidly growing sophistication of cyber-attacks and a lack of data related thereto.

It is obvious that there has been an imminent need to minimize the potential danger of future cyber-attacks, as the IMO, shipowners and the insurers need to be more effective and act fast when trying to eliminate, or, at least, reduce the possibility of cyber losses. Arising, from the conducted research, it is clear, that technological solutions alone will not be not enough to prevent cybercrime. No issues arise if the attack is perpetrated with no damage incurred on the shipowner, however, should this not be the case the party liable for the damage has to be determined. Therefore, the onerous question of who is liable for the damage will arise, as the current insurance policies tend to include numerous exclusion clauses, protecting the insurer from bankruptcy.

In examining these challenges, it was discovered that while the IMO and BIMCO have introduced cyber risk management guidelines aimed at creating cyber risk awareness and cyber risk management, the shipowners still need to comply with these prescribed measures in order to assist the insurers in provision of an affordable cover. The author of this dissertation is of the view, that most appropriate solution to cyber risk is cyber risk insurance coverage that is accessible and affordable for the ship owners. While the initial thought of such sounds rather utopic at the moment, this dissertation illustrates that this scenario can be achieved through incentivization packages, whereby the insurer invisibly enforces the implementation of cybersecurity standards in

exchange of additional benefits, and eventually even lowered premium prices as these directly correlate with the present risk exposure. Following the above drawn mindset, such packages should also target the motivation to report and record the offshore cybercrimes, as the available data and their amount respectively, will lead to increased predictability and accuracy of the risk assessment. By implementation of the above-mentioned tools, the marine insurance industry is likely to achieve a mutually beneficial situation for the insurers as well as their clients, as one hand, the insurers' risk exposure will be decreased, while, on the other, the premium costs to the policy holders will continue to decline.

For the sake of the further improvement and elimination of the cyber insurance gap in maritime industry, the author believe that the insurance policies, guidelines as well as the exclusions thereof, should be streamlined in order to achieve a transparent and client-friendly marketplace where the insurance companies work hand in hand with the policyholders, in order to defeat the common enemy – the emerging trend of cyber-attacks in the maritime industry.

BIBLIOGRAPHY

Books

Baris Soyer *Warranties in Marine Insurance* 3rd edition (2017).

Christoff Luddeke & Contributors *Marine Claims: A guide for the handling and prevention of Marine Claims* (1996).

F.D. Rose Marine Insurance Law and Practice 2nd edition (2012).

John Dunt *Marine Cargo Insurance* (2009).

John Hare *Shipping Law and Admiralty Jurisdiction in South Africa* 2nd edition (2009).

John Lowry, Philip Rawlings & Robert Merkin *Insurance Law: Doctrines and Principle* (2011).

M FB Reinecke, JP van Niekerk & PM Nienaber *South African Insurance Law* (2013).

Malcom A. Clarke *The Law of Liability Insurance* (2013).

Meixian Song *Causation in Insurance Contract Law* (2014).

Neethling Potgieter *Visser Law of Delict* 7th edition (2014).

Prof.D. Rhidian Thomas The Modern Law of Marine Insurance Volume 5 (2015).

Legislation

Insurance Act 2015 (c4) (UK).

Marine Insurance Act 1906.

Cases

Nova Scotia v Hellenic Mutual War Risks Association (Bermuda) Ltd, 'The Good Luck' [1992] 1 AC.

McFadden v Blue Star Line [1905] 1 KB 697.

Moir v Royal Exchange Ass Co (1815) 4 Camp 84.

Thesis

Bilal Ahmad *The Pre-Contractual Duty of Good Faith- A Comparative Analysis in the Marine Insurance Contract Law with the Duty of Good Faith in the General Contract Law* (unpublished LLM thesis, Lund University, 2010) 25.

David Miranda Silgado *Cyber- attacks: a digital threat reality affecting the maritime industry* (unpublished LLM Worlds Maritime University Dissertation, 2018) 33.

Internet Sources

AIG 'Cyber Coverages: Four Steps to Prepare for and Defend Against an Imminent Cyber Attack' available at *https://www.aig.com/business/insurance/cyber-insurance*, accessed on 10 December 2019.

AIG 'Cyber Liability', available at *https://www.aig.co.za/business/products-services/financial-lines/cyber,* accessed on 20 November 2019.

AIG 'CyberEdge® Plus Cyber-attack related bodily injury, property damage, business interruption, and product liability', available at *https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-plus.pdf*, accessed on 20 November 2019.

Allianz Global Corporate & Specialty 'Allianz Risk Barometer 2019:Top Business Risks for 2019' at 4 available at *https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf*, accessed on 06 January 2020.

Allianz Global Corporate & Specialty 'Allianz Risk Barometer 2019:Top Business Risks for 2019' at 5 available at *https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf*, accessed on 06 January 2020

Britannia P&I 'Britannia Streaming Protection & Indemnity Rules and Correspondence Class 3/2019/20' at 49, available at *https://britanniapandi.com/rule-books-for-2019-20-policy-year/*, accessed on 06 January 2020.

Christian Biener, Martin Eling and Jan Hendrik Wirfs 'Insurability of Cyber Risk: An Empirical Analysis. Geneva Papers on Risk and Insurance – Issue and Practice 40.1-28.10.1057/gpp.2014.19 at 12, available at *https://www.researchgate.net/publication/265727415_Insurability_of_Cyber_Risk_An_Empirical_Analysis/citation/download,* accessed on 04 January 2020.

Christian Biener, Martin Eling and Jan Hendrik Wirfs 'Insurability of Cyber Risk: An Empirical Analysis. Geneva Papers on Risk and Insurance – Issue and Practice 40.1-28.10.1057/gpp.2014.19 at 12, available at *https://www.researchgate.net/publication/265727415_Insurability_of_Cyber_Risk_An_Empirical_Analysis/citation*/download, accessed on 04 January 2020.

Dromo Bureau of Shipping 'Guidelines on Maritime Cyber Risk Management' available at *https://maritimecyprus.files.wordpress.com/2018/11/dromon-guidelines-on-maritime-cyber-risk-management.pdf*, accessed on 04 December 2019.

European Insurance and Occupational Pensions Authority *Cyber risk for insurers-challenges and opportunities available at https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf,* accessed on 12 January 2020.

Iris Bajraktari 'Cyber Security and Cyber Risks in the Shipping Industry' Thomas Cooper LLP Publications, 2 May 2019, available at *https://www.thomascooperlaw.com/cyber-security-cyber-risks-shipping-industry/*, accessed on 3 December 2019.

Julian Clark 'Cybercrime in the shipping industry: An overview of the risks and how they apply to you' at available at *http://www.mlasa.co.za/wp-content/uploads/2017/09/Cyber-crime-in-shippinh-Julian-Clark.pdf,* accessed on 19 November 2019.

Lloyd's List' Maritime industry must open up about cyber-crime' available at *https://lloydslist.maritimeintelligence.informa.com/LL1128745/Maritime-industry-must-open-up-about-cyber-crime,* accessed on 06 January 2020.

Lloyd's List' Maritime industry must open up about cyber-crime' available at *https://lloydslist.maritimeintelligence.informa.com/LL1128745/Maritime-industry-must-open-up-about-cyber-crime,* accessed on 06 January 2020.

Marsh 'Cyber Gap Insurance Cyber Risk: Filling the Coverage Gap' at 2, available at *www.oliverwyman.com/content/dam/marsh/Document/PDF/UKen/CyberGapInsuranceCyberRiskFillingtheCoverage,* accessed on 07 December 2019.

Munich Re 'Business interruptions due to cyber events: A challenging cover component' available at *https://www.munichre.com/topics-online/en/digitalisation/cyber/business-interruptions-due-to-cyber-events.html,* accessed on 06 January 2020.

Ruperto P. Majuca, William Yurcik and Jay P. Kesan *The Evolution of Cyberinsurance* Department of Economics: National Center for Supercomputing Applications (NCSA) at 2.

Staff Writer 'Cyber re/insurance market "frustratingly immature"': Inga Beale Lloyd's' in Reinsurance News 27 February 2018, available at *https://www.reinsurancene.ws/cyber-re-insurance-market-frustratingly-immature-inga-beale-lloyds/,* accessed on 9 December 2019.

The Shipowners' Club *Club Rules 2019* at 117, available at *https://www.shipownersclub.com/media/2019/02/Club_Rules_2019_Web.pdf*, accessed on 20 November 2019.

World Maritime News Staff 'In Depth: Cyberthreat Is Here to Stay!' World Maritime News 27 September 2017 available at *https://worldmaritimenews.com/archives/230822/interview-cyberthreat-is-here-to-stay/,* accessed on 1 December 2019.