11-3-2020

Cyber-security risks and liabilities in modern marine insurance.

Thi Hong Hanh Hoang

Cyber security risks and liabilities in modern marine insurance

by Thi Hong Hanh HOANG

Submission date: 28-Oct-2020 03:34PM (UTC+0100)

Submission ID: 134896190

File name: 1748_Thi_Hong_Hanh_HOANG_Cyber_security_risks_and_liabilities_in_modern_marine_insurance_11057_2058574756.docx (290.92K)

Word count: 18334

Character count: 106655

WORLD MARITIME UNIVERSITY

Malmö, Sweden

CYBER-SECURITY RISKS AND LIABILITIES IN MODERN MARINE INSURANCE

By

HOANG THI HONG HANH
Vietnam

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

MASTER OF SCIENCE
in
MARITIME AFFARS

(MARITIME LAW AND POLICY)

2020

Declaration

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

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

(Signature): 

(Date): 22nd September 2020

Supervised by: **Associate Professor Henning Jessen**

Supervisor's affiliation: **Maritime Law and Policy Specialization**

Acknowledgements

It is pride for me to be able to attend and complete MSc. in Maritime Affairs program at World Maritime University (WMU). Nearly passed 18 months, I have acquired the up-to-date knowledge of maritime law and policy as well as professional skills to work in the maritime industry, which I can effectively implement to my country in the near future. On this occasion, allow me to express my gratitude to all of those who have supported me to achieve the final results of studying.

First of all, I would like to thank Korean Government, Ministry of Oceans and Fisheries (MOF) for the full scholarship, which gave me an opportunity to study both MSc. in Maritime Affairs and ESSP programs.

I am grateful for WMU's professors, who taught me in the ESSP program, foundation term, Maritime Law and Policy specialization term with valuable lectures. They really fostered my aspiration of research in the maritime field.

Especially, I would like to express gratitude to my supervisor, Associate Professor Henning Jessen, who guided me from establishing a research proposal to finalizing my dissertation with intensively academic advice, great encouragement and support.

Finally, I sincerely thank my family for their devotion to me. Their belief is great motivation helping me complete this program with all of my dedication.

Hoang Thi Hong Hanh
22nd September 2020

Abstract

Title of Dissertation: **Cyber-security risks and liabilities in modern marine insurance**

Degree: **Master of Science**

This dissertation is a study of cyber-security risks and liabilities for losses and damages caused by cyber-security risks in modern marine insurance. The author overviewed the escalated situation of cyber threats to safety and security of shipping in the maritime industry, examined the approach of IMO and industry organizations relating to cyber risk management, analysed the regulations of Marine Insurance Law 1906 as well as the cyber-related coverage of conventional marine insurance lines (H&M and P&I insurances), and finally suggested a standard Cyber Risk Extension Clause to cover the cyber-security risks as an effective instrument to protect shipowners from the global aggressive cyber threats.

This dissertation argues that the contemporary H&M insurance policies explicitly exclude cyber risks by incorporating the CL380 and the P&I Rules have ambiguity in affirmative exposure of cyber risks. Although the marine insurance market has offered a few options of cyber extension clause; however, the cover is extremely limited, which could not comprehensively protect shipowners against cyber risks.

The suggested Cyber Risk Extension Clause would be consistent in the approach of cyber risk management of IMO, industry organizations and expectations of the marine insurance market. To apply this Clause, the shipowners required to comply with the cyber risk management as a mandatory feature of the safety management system to ensure the seaworthiness of insured ships.

KEYWORDS: Cyber-security risks, Cyber risks, Maritime cyber insurance, Cyber coverage, Cyber insurance liability, Cyber risk extension clause.

Table of contents

List of Abbreviations

AGPS	Allianz Global Corporate and Specialty
AIS	Automatics Identification System
BIMCO	Baltic and International Maritime Council
Britannia P&I	The Britannia Steam Ship Insurance Association Limited
CLIA	Cruise Lines International Association
Company/Companies	means the owner of the ship or any other organization or other such as manager, or the bareboat charters as defined in the ISM Code.
CSIS	Center for Strategic and International Studies
CyRiM project	Cyber Risk Management project conducted by University of Cambridge Centre for Risk Studies
DOC	Document of Compliance
ECDIS	Electronic Chart Display Information System
Gard	Gard P&I (Bermuda) Ltd
GDMSS	Global Maritime Distress and Safety System
GPS	Positioning systems
H&M	Hull and Machinery Insurance
IMO	International Maritime Organization
IACS	International Association of Classification Societies
ICS	International Chamber of Shipping
IFoA	Institute and Faculty of Actuaries
IHC (1/11/03)	International Hull Clause (1/11/03)
INTERCARGO	International Association of Dry Cargo Shipowners
INTERTANKO	International Association of Independent Tanker Owners
IUA	International Underwriting Association of London
IUMI	International Union of Marine Insurance

ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ISM Code	The International Safety Management (ISM) Code or The International Management Code for the Safe Operation of Ships and for Pollution Prevention as, as amended
ISPS Code	International Ship and Port Facility Security Code, as amended
Japan P&I Club	The Japan Ship Owners' Mutual Protection & Indemnity Association
NIST	United States National Institute of Standards and Technology
North	The North of England Protecting & Indemnity Association Limited
MIA 1906	Marine Insurance Act 1906
MLC 2006	Maritime Labour Convention 2006 as amended
OCIMF	Oil Companies International Marine Forum
PRA	Prudential Regulation Authority
P&I	Protection and Indemnity Insurance
Shipowners' Club	The Shipowners' Mutual Protection & Indemnity Association (Luxembourg)
Skuld	Assuranceforeningen Skuld
SOLAS	International Convention for the Safety of Life at Sea, 1974, as amended
SMC	Safety Management Certificate
SMS	Safe Management System
SSA	Ship Security Assessment
SSP	Ship Security Plan
Standard Club	The Standard Club Ltd
Steamship Mutual	The Steamship Mutual Underwriting Association (Bermuda) Limited

The American Club	American Steamship Owners Mutual Protection and Indemnity Association, Inc
The London P&I Club	The London Steam-Ship Owners' Mutual Insurance Association Limited
VDRs	Voyage Data Recorders
VOIP	Voice Over Internet Protocols equipment
UK P&I	United Kingdom Mutual Steamship Assurance Association (Bermuda) Ltd
West	The West of England Ship Owners Mutual Insurance Association (Luxembourg)
WLANs	Wireless networks

CHAPTER I: INTRODUCTION

1.1 Problem statement

Cyber incidents such as cyber attacks, IT failure/outage and data breaches are the top dangerous global business risks. According to the AGPS's report, cyber incidents ranked the second most important business risks in 2018 (40%) and 2019 (37%) while five years ago it ranked 15th (AGPS, 2019). AGPS's report also presents that in 2019, cyber incidents topped risks in the following sectors: aviation, aerospace, defense, entertainment and media, financial services, professional services, technology and telecommunications. In the marine and shipping sector, cyber incidents ranked the second (32%) after natural catastrophes (34%). This position has not changed in comparison with 2018 (AGPS, 2019).

Currently, the maritime industry is making progress in integration, digitalisation, and automation, which significantly contributes to the efficiency of shipping. However, the heavy reliance on advanced technology and internet exposes several challenges. In this regard, the safety and security of ships are critically threatened by cyber risks. A maritime survey conducted in 2018 by BIMCO, ABS Advanced Solution, and Fairplay illustrates that the shipping sector is the major target of cyber attacks with several threats such as phishing, malware, DDoS attacks, ransomware, and others (Fairplay, BIMCO, ABS, 2018). In recent years, the world has witnessed several high-profile cyber incidents at giant global shipping companies as the overwhelming evidence of the maritime industry facing cyber-security risks. Particularly, in 2017, the ransomware called 'NotPetya' destroyed the AP Moller Maersk's computer network (Maersk, 2017). In 2018, the China Ocean Shipping (Group) Company (COSCO) also became a victim of a ransomware attack (World Maritime News, 2018). Most recently, on 9th April 2020, the Mediterranean Shipping Company's website has been down by a suspected malware or dedicated denial

of service (DDoS) attacks (Baker, 2020). More seriously, cyber-security risks have surged during the Covid-19 pandemic with 400% increase in attempted cyber attacks in the maritime and offshore energy sector, according to a report of Naval Dome (Insurance Marine News, 2020). As commented by Jones Walker Attorneys, "*Hackers are modern-day pirates who have the ability to sink maritime industry sectors that are unprepared for what's coming at them*" (Walker, 2018). Therefore, a comprehensive solution to identify, manage, mitigate, and transfer the cyber-security risks should be expeditiously deployed by the maritime stakeholders.

To implement this mandate, over the years, IMO, industrial organizations, classification societies, and marine insurers have made efforts to establish guidelines on cyber security and call for shipowners, ship operators/managers, and other related parties such as agents, vendors, and port managers to apply these recommendations. IMO has issued **Resolution MSC.428 (98) - Maritime Cyber Risk Management in Safety Management Systems**, which requires shipowners to incorporate cyber risk management into the existing safety management system (as defined in the ISM Code). Besides that, in **Circular MSC-FAL.1/CIRC.3 - Guidelines on Maritime Cyber Risk Management**, IMO provides a high-level recommendation to safeguard shipping from cyber risks and vulnerabilities. The group of international shipping organizations led by BIMCO has produced **Guidelines on Cyber Security Onboard Ships**, which provide a risk-based approach to identifying and responding to cyber threats. Meanwhile, IACS has introduced **Recommendation on Cyber Resilience** providing technical requirements to stakeholders that would lead to the delivery of cyber resilient ships and contribute to safe and secure operations. These instruments address cyber risk management as a process of actions from risk assessment (identifying, analysing, assessing, and communicating) to risk treatment (accepting, avoiding, transferring, or mitigating). The objective of this dissertation is cyber risk transfer, which plays an equally important role in a comprehensive cyber risk strategy. Using insurance services is one kind of effective measures to transfer cyber risk.

On the other hand, cyber incidents trigger extensive loss and damage to the global economy in general and the maritime sector in particular. Based on the CISC's statistics,

AGPS reports that the annual damage from cybercrime is estimated at USD 600 billion over the world. This data is three-times higher than a 10-year average economic loss caused by natural catastrophes accounting for around USD 208 billion. However, the average insured loss from a cyber incident is over USD 2.3 million, which is extremely little compared to the loss from the largest event costing hundreds of millions or higher (AGPS, 2019). This data demonstrates that the demand for cyber risk transfer is tremendously high; however, the cyber insurance market is still new and immature. In the maritime sector, the Notpetya malware attack caused the total financial loss to Maersk estimated at nearly USD 300 million (Knowler, 2017). Recently, the CyRiM project has estimated that a computer virus originated by ships could spread to cargo database records at 15 major ports in the Asia-Pacific region, which cost USD 110 billion, equivalent to half of the global losses from natural catastrophes in 2018 (CyRiM, 2019). Experts have suggested that cyber insurance is required to develop as one of the solutions "*to narrow the massive protect gap in cyber risk for the maritime sector*" (Ladbury, 2020).

Along with the actual huge losses and damages, the cyber-security risks and liabilities create challenges to marine insurers from a theoretical perspective. Different from traditional marine insurance products that cover physical losses and damages caused by physical risks, maritime cyber insurance is required to cover modern losses and damages caused by modern risks. Particularly, traditional marine insurance covers, for example, hull or machinery damage caused by a collision accident. However, maritime cyber insurance requires addressing the non-physical loss such as information data loss or reputation damage. Moreover, maritime cyber insurance also needs to cover the physical loss and damage arising from non-physical triggers (HFW, 2016). For instance, a significant loss of a vessel's navigation system may be initiated by a transmission of a virus through malware, which is a non-physical cause. Furthermore, regarding the liability of the indemnity for the third party, the insurers normally indemnify the loss of third party's property; nonetheless, the maritime cyber insurance must deal with the business corruption loss of the third party. For example, the transmission of a virus embedded

email from a shipping company to all suppliers/clients causes a shutdown of their information technology systems and corrupt their business activities.

In addition, the common application of the Institute Cyber Attack Exclusion Clause - CL380 needs the marine insurers to address. In particular, the marine insurers have excluded cyber risks in H&M insurance policies since 2003. Meanwhile, P&I insurance has no explicit exclusion of cyber risks; however, the claims are probably deterred by the argument with P&I Clubs on a case-by-case basis. Analysing the root causes of this problem is a task of marine insurance theory, which could help the maritime sector how to utilise maritime cyber insurance as an effective risk management tool. Furthermore, this also helps marine insurers determine whether to develop a new product of maritime cyber insurance or not as well as to defining the potential coverage of maritime cyber insurance.

Overall, based on the above analysis, three major problems require the necessity of research on the cyber risks and liabilities of marine insurance as following: (i) the rapid increase of cyber-risks jeopardizing the maritime industry and the demand of the maritime sector on protection against cyber risks; (ii) the theoretical complexity of cyber insurance's coverage; and (iii) the lack of clarification on cyber risks coverage of traditional marine insurance products and the practical implementation of the cyber-risks exclusion clauses.

1.2 Literature review

For a literature review in terms of cyber risks and liabilities of modern marine insurance, there are three main research groups. The first group studies cyber security in the maritime industry; the second group explores cyber insurance as a kind of new product applied for all business sectors; the third one examines the cyber risk insurance in the maritime domain.

Firstly, the research of cyber security in the maritime industry provides knowledge of cyber safety and cyber security in terms of technical and operational perspectives. There are numerous published articles as well as theses on this topic. For example, Oliver Daum in the article **"Cyber security in the maritime sector"** provides an overview of relevant IT structures of the maritime industry and explains how hackers gain access to

IT systems. The author analyses the current state of the international law of cyber security and refers to the impact of cyber risks when lacking the preventive measures, especially to unmanned shipping (Daum, 2019). Kimberly Tam and Kevin Jones have produced a paper, **"Factors affecting cyber risk in maritime"**, which explores the full range of factors affecting cyber-related risks in the maritime sector to evaluate applicable risk frameworks and suggest the improvement of cyber risk assessment tools (Tam & Jones, 2019).

Secondly, the research of cyber insurance investigates the nature of cyber risk and liability; however, the scope of research broadens to all of sectors using information technology, not only the maritime sector. For instance, in the article **"Cyber risk and the changing role of insurance"**, the meaning of cyber risk is introduced from the insurance perspective, the necessity of cyber insurance in the future is predicted, and organizations are encouraged to implement a safety management system to mitigate cyber risk (Camillo, 2017).

Lastly, the remaining group proposes the research of the relationship and correlation between cyber security in the maritime industry and cyber insurance. (Cooper, 2019) presents the nature of cyber risk faced by the shipping industry, the means of attack, the source of risk, industry and regulatory response, and the insurance implications. In addition, Soyer provides an overview of the cyber risks insurance market, analyses cyber risk coverage, and examines the cyber exclusions. The research suggests that maritime companies should appreciate the scope and nature of cyber risk policies available and the relationship between these policies with traditional insurance products to be effectively protected against cyber risks (Soyer, 2020). In 2018, Davit Dadiani completed the Master degree's dissertation with the topic **"Cyber security and marine insurance"**. He explores current approaches of marine insurance regarding cyber security through reviewing the cyber risk coverage of marine insurance. The study analyses the current international legal framework regulating cyber-security in marine insurance and suggests the measures that marine insurers can deal with the cyber-attacks (Dadiani, 2018).

Previous research contributed to establishing the foundation of cyber security in the maritime industry, the theory of cyber risk and liability, the necessity of cyber insurance in the maritime industry, and the legal framework of marine insurance in terms of cyber security. However, the research merely suggested general principles but has not yet recommended specific amendments or supplementations of the legal framework to maritime cyber insurance. Meanwhile, no prior literature proposes a new standard clause for cyber insurance in the maritime industry.

1.3 Aims and objectives

To fill the above gaps, this research aims to:

- Explore traditional marine insurances (H&M insurance and P&I insurance) at risk and liability perspectives.
- Analyse the nature of cyber risk and liability, which should be covered by maritime cyber insurance.
- Analyse the marine insurance law and traditional marine insurance clauses/rules to define the legal barriers/shortages/conflicts of maritime *c*yber insurance.
- Analyse the necessarily required conditions to implement maritime cyber insurance.

1.4 Research questions

To conduct the research objectives, the research questions are posed as follows:

- What is the nature of cyber-security risks?
- What are the kinds of losses and damages caused by cyber-security risks?
- What liabilities should be covered by marine insurers for the losses and damages caused by cyber-security risks?
- Does MIA 1906 need to be amended to regulate the cyber-security risks and liabilities or could new risks and liabilities still be covered under the current regulations? If the amendment is necessary, how should MIA 1906 be revised?

- What factors influence the implementation of maritime cyber insurance?

1.5 Methodology

The research was mainly conducted by the legal research method and analytical research method. For the practical research, the following methods were used:

(1) ***Documentary review:*** the research reviewed books, articles, journals, publications, websites, reports, and other reliable sources to find the supporting evidence and convincing arguments for reference.

(2) ***Legal research:*** the research reviewed and analysed legal documents to define the gaps of the current legal system in terms of research topic and proposed the amended or new regulations to fill the gaps.

(3) ***Case study:*** the research collected and analysed the cyber-related case studies in the maritime industry which made it possible to illustrate the nature of cyber risk and liability.

(4) ***Comparative research:*** the research compared the marine insurance policies or rules between different marine insurers to find the best solution to potential marine cyber insurance clauses in the future.

1.6 Expected results

The research expects to contribute these results:

- Suggestions for particular amendments of MIA 1906 in terms of cyber-security risks and liabilities (if any).
- Suggestions for a new maritime cyber insurance clause applied for H&M insurance and P&I insurance.
- Suggestions for maritime safety conditions/requirements to ensure maritime cyber insurance clauses could be implemented in reality.

1.7 Potential limitations

This research made efforts to present and analyse the convincing and rational opinions/arguments to get the expected results. However, there are several limitations as follows:

- This research focuses on the cyber risks in shipping transactions, excluding cyber-threats in ports, supply chains, or other maritime activities.
- This research analyses the cyber risks and liabilities relating to H&M insurance and P&I insurance, excluding cargo insurance; freight, demurrage and defence insurance; or the other one.
- This research explores the legal perspective but does not analyse the economic perspective of marine cyber insurance.
- This research does not study the technical and operational aspects of cyber security.
- The data limitation of cyber security and cyber attacks from shipping companies and authorities may restrict the potential outcomes of this research.
- The confidential clauses in insurance policies may limit the information from the insurers of this research.

CHAPTER II: CURRENT APPROACHES OF CYBER-SECURITY RISKS IN MARITIME SAFETY AND SECURITY

Numerous last decade cyber incidents have awakened the maritime industry to become aware of cyber risks threatening both the safety and security of shipping. The establishment of a comprehensive solution to avoid and mitigate cyber incidents is a challenging mandate for maritime stakeholders. As a United Nations specialized agency, IMO is a policy-maker in developing the regulatory framework to tackle cyber risks in the maritime arena. IMO has elaborately examined the scopes and objectives of existing instruments relating to maritime safety and security to decide an appropriate approach being able to deal with cyber risks at present. This chapter reviews the ISM Code, the ISPS Code, the IMO's guidelines, and the industrial guidelines to depict an overview of current approaches to cyber risks in the maritime industry.

2.1 International Safety Management (ISM) Code

The ISM Code is an incorporated part of Chapter IX of SOLAS. Its purpose is "*to provide an international standard for the safe management and operation of ships and for pollution prevention*"[1]. To accomplish this purpose, the objectives of the Code are established to ensure safety at sea, prevent human injury or loss of life, and avoid damage to the environment and property. The Code sets the Company's fundamental safety management objectives including the assessment of all *"identified risks"* to its ship, personnel, and the environment as well as the establishment of appropriate safeguards. The Code requires every Company to develop, implement, and maintain a safety management system (SMS), which is a structured and documented system of policies,

[1] Paragraph 1 Preamble of ISM Code (ISM Code, 1998)

instructions, procedures, and plans enabling the Company to achieve a safe and efficient ship operation. The SMS should satisfy the fundamental requirements including:

(i) a policy of safety and environmental protection;
(ii) instructions and procedures to ensure the safe operation of ships and protection of the environment;
(iii) the authority levels and communication lines between ship-shore personnel;
(iv) procedures for reporting accidents and non-conformities;
(v) procedures to prepare for and respond to emergency situations;
(vi) procedures for internal audits and management reviews.

For a long time, the *"identified risks"* term in the ISM Code is traditionally recognized as the physical threats. Administrations, classifications and societies, port state controls, Companies and other stakeholders implemented the ISM Code to deal with physical threats, not to digital ones. Recently, the IMO's Maritime Safety Committee adopted Resolution MSC.428 (98) on 16 June 2017 with the title **"Maritime Cyber Risk Management in Safety Management Systems".** This is a crucial document to confirm that cyber risks should be managed as an additional kind of identified risks, and maritime cyber risk management should be a complementary part of the SMS in accordance with the objectives and functional requirements of the ISM Code. Meanwhile, IMO encourages administrations to establish the measures to Companies to undertake the maritime cyber risk management in the SMS before the first annual verification of the Company's Document of Compliance (DOC) after 1 January 2021. The IMO's approach of cyber risk management is non-mandatory application; however, this is the foundation to increase authorities', shipping companies', and seafarers' cyber security awareness.

2.2 International Ship and Port Facility Security (ISPS) Code

The ISPS Code is an associated part of Chapter XI-2 **"Special Measures to Enhance Maritime Security"** of the SOLAS. The main objective of the Code is "*to*

establish an international framework … to detect/assess security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade…"[2]. Traditionally, the focus of the ISPS Code is on physical security threats such as piracy, maritime terrorism, armed robbery against ships, and other acts of maritime violence. However, external threats such as cyber crimes, cyber attacks, and other malicious actions (e.g. hacking or introducing malware) are security threats because they jeopardise the ships' security. Indeed, the requirements of assessments and measures under the ISPS Code are necessary to protect ships against cyber threats. The ISPS Code requires Companies to carry out appropriate measures to identify and prevent security incidents. These measures include acting upon security levels (section 7), implementing the ship security assessment (SSA) (section 8), and complying with the approved ship security plan (SSP) (section 9). The SSA has to address the element of *"identification of possible threats to the key shipboard operations"* (section 8.4.3 Part A), and should take into account the *"radio and telecommunication systems, including computer systems and networks"* which pose risk to ship operations (section 8.3.5 Part B). Furthermore, the measure of physical security could prevent unauthorised physical access to the ship's technology infrastructure. In this regard, the technology systems of the ship should be taken into account as the restricted areas required to be identified and protected according to the SSA and the SSP (MSC101/4/4, 2019).

Resolution MSC.428 (98) affirms that raising awareness on cyber threats and vulnerabilities is imperative to enhance both safe and secure shipping. However, at the 101st session, the IMO's Maritime Safety Committee and the co-sponsors (the United States, ICS, BIMCO) recognised that incorporating cyber risk management into the SMS instead of establishing a separate cyber security management operating under the ISSP Code is the proper measure to avoid the administrative burden to Companies. In addition, the SSP should not be a repository of cyber security procedures because the burden and cost will land on Companies when any change of SSP requires the Administration's approval as the cyber security is rapidly developed and frequently updated (MSC101/4/4,

[2] Foreword of ISPS Code (ISPS Code, 2004)

2019). It is notable that the Maritime Safety Committee continuously considers these concerns.

2.3 IMO Guidelines on Cyber Risk Management

In 2017, IMO issued the Circular MSC-FAL.1/CIRC.3 - **Guidelines on Maritime Cyber Risk Management**, which provides a high-level recommendation to safeguard shipping from cyber threats and vulnerabilities. The guidelines introduce a cyber risk management approach in broad terms as fundamental principles to have flexible applications in each Company. Article 1.1 of the Guidelines presents the definition of maritime cyber risk:

> *Maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety, or security failures as a consequence of information or system being corrupted, lost or compromised.*

The technology asset in the context of the Guidelines could be classified into information technology (IT) systems (including information and data) and operation technology (OT) systems. IT systems are devices, equipment and appliance using data to control, whilst the OT systems utilise data to control or monitor physical processes. The IT system includes IT networks, email, software or application of administration, accounts, crew lists, planned maintenance, spares management and requisitioning, electronic manuals and certificates, permits to work, charter party, a notice of readiness, bill of lading. The OT system comprises but is not limited to the Electronic Chart Display and Information Systems (ECDIS), Global Positioning Systems (GPS), marine Automatic Identification Systems (AIS), remote supports for engines, data loggers, engine and cargo control and dynamic positioning. Both IT and OT systems explore the dangers to the ships, which are called vulnerable areas. Article 2.1.1 regulates the vulnerable systems, which could include but are not limited to:

(i) *Bridge systems*
(ii) *Cargo handling and management systems*
(iii) *Propulsion and machinery management and power control systems*
(iv) *Access control systems*
(v) *Passenger servicing and management systems*
(vi) *Passenger facing public networks*
(vii) *Administrative and crew welfare systems*
(viii) *Communication systems.*

The cyber risks may arise from inadequate operation, integration, maintenance, and design of IT or OT systems, and from intentional and unintentional threats, which lead to the safety and security impacts on the ship, personnel, environment, the Company, and cargo.

To safeguard safe and secure shipping operations, Companies should develop and implement cyber risk management, which is incorporated into the SMS as suggested by the MSC.428 (98). Article 3.1 regulates:

> *Cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.*

This process requires a holistic and flexible regime based on the financial ability and desired outcome of the Company. A cyber risk management plan should be made and taken into account the risk management objectives and the allocation of resources in the most effective manner. In addition, the framework of cyber risk management should embrace five functional elements: identify, protect, detect, respond and recover. The vulnerabilities of the ship should be identified and the person who is responsible for cyber

risk management should be designated. The Guidelines emphasise the increase of cyber risk awareness from the senior management level to all personnel of the Company. This is an indispensable element of effective maritime cyber risk management.

Overall, the framework of cyber risk management in MSC-FAL.1/Circ.3 is the foundation for maritime actors to intensively understanding cyber threats, ship's vulnerabilities and the procedures to manage cyber risks. To implement the Guidelines precisely, IMO suggests that the Company should apply the Member Governments and Flag Administrations' requirements, as well as the standards and best practices of industrial organizations. From 1 January 2021 onwards, the cyber-related safety management system will be verified under internal audit and ship-based survey procedures as a mandatory requirement. Any identified omissions of cyber security, weaknesses and deficiencies in cyber-related safety management system might lead to unseaworthiness or non-compliance of the ship. This could cause serious legal consequences not only fines or detentions by port state controls but also contractual disputes relating to charter parties, contract of carriage of goods, and potential failure of insurance claims.

2.4 Industrial Guidelines on Cyber Risks Management for the Maritime Sector

In 2018, a group of international shipping organizations including BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF, and World Shipping Council developed the **Guidelines on Cyber Security Onboard Ships** version 3.0 (hereafter called the Industrial Guidelines) to mitigate the cyber incidents and consequences arising from these events. The Industrial Guidelines provide a risk-based approach that enables Companies to identify and respond to cyber threats as well as to effectively applying resources in cyber risk management.

The cyber risk management in the Industrial Guidelines is developed from the framework of the cyber risk management with five functional elements embracing the following: identify, protect, detect, respond, and recover as defined under the MSC-

FAL.1/Circ.3. Based on this framework, six components are improved for a comprehensive cyber risk management under the Industrial Guidelines, namely:

(i) Identify threats
(ii) Identify vulnerabilities
(iii) Assess risk exposure
(iv) Develop protection and detection measures
(v) Establish contingency plans
(vi) Respond to and recover from cyber security incidents.

Especially, the 6th component of responding to and recovering from cyber security incidents provides the recommendations relating to losses arising from a cyber incident and the insurance cover for property damage and liability. Furthermore, there are seven incidents introduced and analysed to illustrate each component. Annex 2 of the Guidelines is designed to provide the minimum measure, which assists Companies to incorporate the cyber risk management into their existing approved SMS.

Notably, the Industrial Guidelines are aligned with Resolution MSC.428 (98) and IMO's Guidelines MSC-FAL.1/Circ.3. They offer practical recommendations on both cyber security and cyber safety in the maritime sector. This instrument suggests that the Company's cyber risk management programme should take into account the requirements of both existing SMS and SSPs according to the ISM Code and ISPS Code.

2.5 IACS Recommendation on Cyber Resilience No.166

In April 2020, IACS published the Recommendation on Cyber Resilience No.166, which was consolidated by previous 12 Recommendations concerning cyber resilience (from No.153 to No.164). This instrument provides technical requirements in design, construction, and testing of onboard computer-based systems to deliver and maintain cyber resilient ships[3]. The Recommendation uses the goal-based approach and the goals

[3] Article 1.1.1; 2.1; 2.4 and 5.1 of the IACS No.166

were drafted according to 5 elements of effective cyber risk management introduced in IMO Guidelines[4], including:

(i) **Identify:** Completely understand all the devices, systems, networks and data flows on board;

(ii) **Protect:** Harden systems and devices, to protect the OT systems and relevant information as effectively as possible;

(iii) **Detect:** Timely and effectively detect the cyber incidents;

(iv) **Respond:** Limit the effects of damage to OT systems and relevant information as much as possible;

(v) **Recover:** Timely restore the OT systems to maintain the ship's safe condition.

To implement these goals, the Recommendation provides the functional requirements (section 6), technical requirements (section 7), provisions of verification testing (section 8), which should be applied by maritime stakeholders. This important document supports IMO Resolution MSC.428 (98) in technical perspective[5] and marks a significant step in addressing cyber resilience from the vessel's design stage (IACS, 2020).

In conclusion, the cyber-security risks endanger both the safety and security of shipping. The regulatory and industry regime of cyber security onboard ships is in the process of formation and development; however, it is the fundamental framework to assist the maritime industry to combat cyber-security risks. In addition, it is the cornerstone to support marine insurers to examine cyber-security risks and liabilities and develop the proper maritime cyber insurance products, which are discussed in the following chapters.

[4] Article 5.2 of the IACS No.166
[5] Article 1.1.5 of the IACS No.166

CHAPTER III: CYBER-SECURITY RISKS IN MODERN MARINE INSURANCE

The purpose of this chapter is to identify what cyber-security risks are in comparison with the definition of the "maritime risks" according to the Marine Insurance Act 1906 (MIA, 1906) to determine whether cyber-security risks are a kind of maritime risk. Besides, this chapter reviews the insured risks of contemporary H&M and P&I insurance policies to analyse whether cyber-security risks have any possibility to become the insured risks according to these policies. Several examples will be examined to illustrate the nature of cyber-security risks during the discussion.

3.1 Insured risks in the Marine Insurance Act 1906

The MIA 1906 is a legal foundation of marine insurance law, which was codified from established case law related to the relationship between the parties to a contract of marine insurance in England during the eighteenth and nineteenth centuries. Currently, this Act is a crucial principle to establish marine insurance policies and become a model to marine insurance law of many countries in the world. The subject-matter of marine insurance is at risk from maritime perils (Thomas, 2009) as defined by section 3.2 of the MIA 1906:

> *"Maritime perils"*[6] *means the perils consequent on, or incidental to, the navigation of the sea, that is to say, perils of the seas, fire, war perils, pirates, rovers, thieves, captures, seisures, restraints, and detainments of princes and peoples, jettisons,*

[6] The words "peril" and "risk" are interchangeable meanings to describe the situation of hazards or losses to which a marine adventure may be exposed (Rose, 2012).

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

This definition introduces a typical feature of maritime perils that is "consequent on" or "incidental to" the navigation of the sea. It also gives an open list of the maritime perils, which is not limited by several tangible risks but includes the opportunity to supplement other risks by the particular insurance policy. Furthermore, according to the principle of MIA 1906, a maritime peril only becomes an insured risk when (i) it is named at a list of perils in a particular insurance policy; (ii) it proximately causes the loss, and (iii) it is not subject to an exclusion[7]. The insured risks under traditional approaches to H&M and the P&I insurance policies will be examined, as shown below.

3.2 Insured risks in contemporary marine insurance policies

3.2.1 Hull and Machinery Insurance

H&M is a property insurance where a ship is an insured subject. The insurance market introduced several H&M insurance policies such as Institute Time Clause (Hulls) (1/10/83), Institute Time Clause (Hulls) (1/11/95), and International Hull Clause (1/11/03). This chapter looks at the third one - International Hull Clause (1/11/03) to review Clause 2 of the perils, which the ship is insured against.

The perils are grouped into two categories of risks, in which Clause 2.1 covers the marine risks and Clause 2.2 covers the Inchmaree risks as explained below.

a. Marine risks

Marine risks consist of the traditional perils to be found in most marine insurance contracts, they are as follows:

[7] Article 55, MIA 1906

- **Perils of the sea:** This refers to fortuitous accidents or casualties of the sea such as rough weather, grounding and stranding, collision, and incursion of seawater but excludes the ordinary action of the winds and waves[8].
- **Fire and explosion:** The insurer will cover for the loss proximately caused by fire, even if the fire was triggered by negligence, barratry, a justifiable deliberate act or arson (Rose, 2012).
- **Theft:** The violent theft by persons from outside the vessel means the theft is not clandestine and must be committed by one or more outsiders. Anyone of the ship's company, whether crew or passengers are not accounted perpetrators of a theft[9].
- **Jettison:** This refers to the deliberate throwing overboard of property for the safety of vessels and the common benefit of related parties in an emergency.
- **Piracy:** Piracy is a forcible robbery at sea, whether is the open sea or territorial water (Gurses, Hjalmarsson, & Pilley, 2014). The term “pirates” includes passengers who engage in mutiny and rioters who attack the ship from the shore[10].
- **Contact with fixed and movable objects:** The IHC (1/11/03) covers for loss and damage caused by contact with fixed objects including land conveyance, dock, or harbor equipment or installation and/or contact with floating objects embracing satellites, aircraft, helicopters or similar objects, or objects falling therefrom.
- **Natural forces:** The standard marine insurance clauses do not provide cover for losses caused by all events of natural forces, but only insure against earthquakes, volcanic eruptions and lightning.
- **Cargo handling:** The assured can recover the loss caused by accidents in loading, discharging or shifting cargo, fuel, stores or parts.

[8] MIA Schedule 1 Rule 7
[9] MIA, Schedule 1 Rule 9
[10] MIA, Schedule 1 Rule 8

b. Inchmaree risks

This group of risks covers additional perils, which are called the Inchmaree clause originated from the particular case of a vessel suffering an explosion in a boiler, embracing:

- **Bursting of boilers or breakage of shafts:** The loss and damage to the ship caused by bursting of boilers or breakage of shafts will be covered by the insurer; however, the insurer only covers a half of the common cost for repairing the boiler or the shaft and the damage caused by them[11].
- **Latent defect:** A latent defect is a deficiency in the machinery or hull that could not be identified by a skilled and due diligent man during the examination. The insurer is only liable for half of the common cost for correcting the latent defect and the damage caused by it[12].
- **Negligence:** The IHC (1/11/03) covers losses caused by "negligence of Master, Officers, Crew or Pilots" as well as "negligence of repairers or charterers", but the negligence of assured itself is not covered[13].
- **Barratry:** According to the MIA Schedule 1 Rule 11, barratry is any wrongful act willfully committed by the master or crew to the prejudice of the shipowner or charterer.

3.2.2 Protection and Indemnity Insurance

P&I is third party liability insurance for shipowners, which is provided by the P&I Clubs. P&I Clubs are mutual, non-profit-making insurance associations of shipowners engaged in the insurance of marine risks embracing protection risks, indemnity risks, or

[11] Clause 2.1.1 and Clause 2.3 IHC (1/11/03)
[12] Clause 2.1.2 and Clause 2.4 IHC (1/11/03).
[13] Clause 2.2 of IHC (1/11/03) regulates that this insurance covers loss of or damage to the subject-matter insured caused by the Inchmaree risks "provide that such loss or damage has not resulted from want of due diligence by the Assured, Owners or Managers". In the context of Inchmaree clause, "want of due diligence" is a lack of reasonable care (Gurses, 2015).

any risks in either or both categories (IGP&I, 2019). The difference between protection risks and indemnity risks depends on academic stance. One point of view reveals that protection covers liabilities to personnel and for damage to property, while indemnity covers liabilities to cargo owners under a carriage contract (Gurses, Hjalmarsson, & Pilley, 2014). Another opinion argues that the “protection” element covers the shipowner’s liabilities deriving from the ownership of the vessel whilst “indemnity” refers to the liabilities for risks related directly to the ship's operation (Donner, 2016). Generally, P&I risks are synthesised as follows (Gurses, Hjalmarsson, & Pilley, 2014):

- *liabilities to passengers, crew or others, for personnel injury and death claims and including cancelled voyages*
- *medical treatment and repatriation of sick, injured or deceased crew members*
- *crew unemployment indemnity following a casualty*
- *claims for loss or damage to cargo*
- *damage to fixed and floating objects*
- *unrecoverable General Average contributions*
- *stowaways*
- *collisions – 25 percent of damages payable to the colliding vessels*
- *liabilities under approved towage contracts*
- *wreck removal*
- *expenses of marine inquires*
- *expenses incidental to the operation of ships – subject to direction of the club directors*
- *special compensation under the 1989 Salvage Convention*
- *fines; including those for pollution*
- *civil liability for pollution.*

The particular covered risks are presented in the Rules of each P&I Club. In this short overview of P&I insurance, it is not possible to analyse individual risks in detail. The

Appendix 2 of this dissertation introduces Part II - P&I Cover in Rules for Ships 2020 of Gard for reference (Gard, 2020).

3.3 Cyber-security risks in modern marine insurance

3.3.1 Definition of cyber-security risk

The definition of risk fundamentally revolves around the qualitative and quantitative likelihood of an accident or unplanned event occurring, considered in conjunction with the potential consequences of such a failure (DNV-GL, 2016). This means a particular event probably occurs or will happen leading to the explicit or implicit consequences. The qualitative and quantitative elements are taken into account as the frequency and measure (high, medium, and low impact) of risk.

The cyber risk is defined as the risk of any financial loss, disruption, or negative reputational impact because of a failure in information technology systems; whether through people, processes, or technology (IFoA, 2019). Based on the definition of risk, it is understood that the cyber risk is a potential accident or event that may result in information technology system failures, which lead to the consequences of financial loss, disruption, or negative reputational impact.

In the maritime sector, according to IMO, the maritime cyber risk is a potential circumstance or event that threatens a technology asset that may cause the information or system to be corrupted, lost, or compromised leading to the failures of shipping operations, safety and security.

These definitions are the background to analyse the nature of cyber risks in the maritime industry and to identify insured maritime cyber risks. Based on the above analysed principle of marine insurance, a maritime cyber risk will be considered as an insured maritime peril when it occurs and causes the explicit loss or damage relating to the operation of ships. Therefore, identifying the maritime cyber risk coverage in comparison with the coverage of conventional marine insurance policies is one of the main objectives of this dissertation. To start, the following sections will analyse the nature of cyber-security risks in marine insurance through the categories of the cyber-security

risks and losses or damages arising from them. Numerous case studies and scenarios of incidents[14] relating to both ship and Company operations will be examined as follows:

3.3.2 Categories of cyber-security risks

Cyber-security risks in the maritime sector can be categorised by various ways consisting of:

(i) onboard and onshore cyber risks
(ii) cyber risks arising from the use of IT and OT system onboard
(iii) intentional and unintentional cyber risks
(iv) cyber risks arising from external factors and internal factors
(v) cyber risks resulting in cyber security incidents and cyber safety incidents
(vi) cyber risks presented by malicious actions and non-malicious actions.

Indeed, the combinations of various classified criteria should be considered to acquire a comprehensive awareness of cyber-security risks; however, the fundamental perspective is the malicious actions and non-malicious ones.

a. Malicious actions

Malicious actions are the deliberately wrongful acts presenting cyber risks and committed by any individual(s) or organization(s) whether externally or internally involved in ship or Company operation that result in or potentially result in loss or damage to the ship or the Company. The malicious actions arising from external factors and internal factors are respectively introduced as follows:

[14] The scenarios analysed in this thesis are introduced by the Guidelines on Cyber Security Onboard Ships version 3.0 (BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF, and WORLD SHIPPING COUNCIL).

- **External factors:**

Cyber attackers represent the overwhelming danger of the shipping industry. They may come from various sources including organised criminals, political activists, competitors, amateur hackers, states, states sponsored organisations and terrorists. According to IACS Recommendation No.166, a cyber attack is "*any type of offensive maneuver that targets IT and OT systems, computer networks, and/or personal computer devices and attempts to compromise, destroy or access Company and ship systems and data*". Cyber attackers may use several different untargeted and targeted devices to attack ships or Companies.

The typical untargeted attacks including:

Malware: Malware is combined by two words malicious and software, which exists under various types such as viruses, worms, spyware, ransomware, and trojan. Malware is designed to use software or codes to access or damage a computer without an unknown owner through exploiting the deficiencies and technical problems of the computer, for example, outdated business software or hardware malfunction. Ransomware can encrypt data to request a payment for ransom. Malware could cause the disruption of the IT infrastructure of a Company, or loss of control a part or all of the ship's OT systems.

In 2017, Maersk was an unintended victim of a state-sponsored cyber attacker. The NotPetya ransomware entered the Maersk's accountancy system in the Ukraine, irreversibly encrypted the computer master boot records, and rapidly spread across the organization. The ransom demand was only $300 in bitcoin; however, the key to restoring the data did not exist because the attackers' goal was purely destructive. Though computers on the fleets of Maersk were not impacted, the repercussions were immense at a global scale. The ships could not load or unload containers because the terminal software was entirely wiped out and electronic cargo manifests could not be received by the ports (BIMCO, 2019).

Phishing: This popular means of attack is deployed by sending emails to wide-ranging potential targets hunting for passwords, inviting a victim to visit a fake website

via a hyperlink, or download a document. Data could be stolen and malware could be spread via phishing.

On 27th October 2019, the MT Eleanna - a Panama flagged oil and chemical tanker received a malicious email with the subject ***"Delivered: Re: M/T Eleanna"***. The analysis reveals that this malicious email was sent to multiple domains to attempt to deliver a popular banking Trojan malware. One of the targeted domains is the website of AmosConnect Software, which is an email service that uses satellite connections for communication to serve the maritime industry on board ship. The potential victims of this attack could be vessels, port facilities, and shore companies in the maritime, oil and gas supply chain (DG, 2019).

Water holing: This type of attack is creating a fake website or deteriorating the genuine one to upload malware on to tricked visitors' systems.

The targeted attacks may utilise these following methods:

Social engineering: The attacker, via social media, exploits individual seafarers or shore base employees to insert malware into the system or reveal confidential information. According to the North of England P&I Association, in 2016 a HudsonAnalytix's client suffered a direct loss of more than USD 250,000 because an employee was tricked by social engineering that caused a series of fraudulent transactions to the criminals (North, 2017).

Brute force: The attacker systematically tests numerous passwords to predict the correct one to access the system and steals the data or delivers the malware. For instance, the ship's IT infrastructure was infected by ransomware resulting in critical files on the server to be locked; the confidential data was lost and administrative software was inoperative. The root cause was poor password policy on the ship allowing attackers to use brute remote force successfully[15] (BIMCO, 2018).

Denial of service (DoS): A distributed denial of service attacks dominates a targeted computer system or server by overwhelming data. The legal users are prevented

[15] Incident: Main application server infected by ransomware

from accessing the information mainly due to the attacker's motivations for commercial sabotage, revenge, or blackmail.

Spear-phishing: This contrivance is like phishing but the targeted victims are individuals. The emails with malware, harmful links, or fraud information are sent to the personal email address in an attempt to discover details of cargo or persuade to wire transfer to the fraudster's bank.

On 27th October 2019, the MV Tasmanic Winter - an American flagged general cargo ship was the intended attack via the malicious email with the subject ***"Request PDA-MV Tasmanic Winter-V075/Discharging"*** requesting shipping documents. It appeared to be a legitimate email; however, it contained Trojan virus (DG, 2019).

- **Internal factors:**

The disgruntled employees or seafarers may threaten the ship and Company by utilising one of the tactics as introduced above or inserting their own devices with malware to harm the IT and OT systems.

b. Non-malicious actions

Non-malicious actions are unwitting acts presenting cyber risks and committed by any individual(s) or organization(s) whether externally or internally involved in ship or Company operation that result in or potentially result in loss or damage to the ship or the Company. The malicious actions also arise from external factors and internal factors.

- **External factors:**

Agents, vendors (manufacturers, equipment suppliers, terminals, port services vendors), ship visitors (surveyors, port state control authorities).

Agents: Agents play an important role in the supply chain as the shipowner's representatives. They are coordinators between related stakeholders to arrange the ship's call port and logistics services. Agents' IT systems are also targeted victims of attackers due to their wide-range networks of business and their principal in the global

and local supply chain. A ship or Company could be indirectly infected with malware from unwitting agents by the electronic information exchanges via IT systems. In this scenario, a shipowner's business network was infected with ransomware via an email attachment. The ransomware came from two unwitting ship agents, in separate ports, and on separate occasions. Ships were also impacted with inconsiderable damage while navigation and ship operations were unaffected. The shipowner paid the ransom in one case[16] (BIMCO, 2018).

Vendors: During business operation, Companies establish contract transactions with multiple vendors such as shipyard, equipment manufacturer or supplier, fuel supplier, crew manning agency, terminal and port services vendor, etc. The weakness of the cyber security of a vendor's products or infrastructure may result in cyber incidents with corporate IT systems or IT/OT systems of the ship. The following scenario illustrates that a ship's power management system, although it was not connected to the internet by design, discovered a dormant worm virus had been in the system for 875 days. It could have activated itself if the system had been connected to the internet and have had severe consequences. An investigation proved that the technical service provider delivered the malware into the ship's system via a USB device during a software installation[17] (BIMCO, 2018).

Visitors on board: Visitors such as surveyors and port state control authorities are cyber dangers with their device potentially containing malware. For instance, when a dry bulk vessel had just completed bunkering operations, the bunker surveyor boarded the ship and inserted his USB device into a computer at the engine control room to print documents for signature. He unintentionally introduced malware onto the ship's administrative system[18] (BIMCO, 2018).

[16] Incident: Ship agent and shipowner ransomware incident
[17] Incident: Worm attack on maritime IT and OT
[18] Incident: Bunker surveyor's access to a ship's administrative network

- **Internal factors:**

Seafarers and onshore employees use their own devices and peripherals including smartphones, tablets, laptops, memory sticks and portable hard drives, so they also innocently introduce malware into the ship and Company systems.

c. Weakness or vulnerability in systems

In addition to the malicious and non-malicious actions, the inherent weakness of IT and OT systems could result in cyber risks. It typically stems from misconfiguration of equipment and software, from software design, or updates containing undetected weakness causing insufficient verification and validation of the software (DNV-GL, 2016). These weaknesses are precisely cyber vulnerabilities onboard existing ships and on some newbuildings, which are presented by industrial experts in the IMO Guidelines (MSC-FAL.1/Cir.3, 2017), consisting of:

- *obsolete and unsupported operating systems*
- *outdated or missing antivirus software and protection from malware inadequate security configurations and best practices, including ineffective network management and the use of default administrator accounts and passwords*
- *shipboard computer networks, which lack boundary protection measures and segmentation of networks*
- *safety critical equipment or systems always connected with the shore side*
- *inadequate access controls for third parties including contractors and service providers.*

The following scenario can demonstrate this point. A ship suffered a failure of nearly all navigation systems at sea because all ECDIS computers were unable to run the updated navigation software. The root cause of this issue was outdated operating systems. At the previous port call, a producer's technician performed a navigation

software update on the ship's navigation computers. However, the outdated operating systems were incapable of running the software and crashed[19] (BIMCO, 2018).

Indeed, the malicious and non-malicious actions not only expose but also exploit weakness or vulnerability of IT and OT systems to trigger the cyber risks. Conversely, the weakness or vulnerability of the system can trigger the cyber risks by itself.

In summary, based on the nature of cyber-security risks, it could be generalized that cyber-security risks are: (i) unauthorised access, manipulation, disruption, and failure of the IT and/or OT system; (ii) failure or loss of availability or integrity of the IT and/or OT system; (iii) loss of availability, integrity, or confidentiality of information and data of a ship or a Company.

3.3.3 Loss or damage arising from cyber-security risk

Like natural catastrophes, cyber-security risks may also result in physical effects and/or pollution incidents as well as significant loss of business. In the maritime context, the loss or damage arising from cyber risks should be considered from the perspectives of ship operation and Company operation.

a. Loss or damage relating to ship operation

It may be said that a ship is the most valuable but also the riskiest asset of a shipowner. During the marine adventure, several risks may cause the loss of and damage to the ship, crew, cargo, and environment. Cyber risks also attribute to these consequences, consisting of:

- **Property damage:** A cyber incident may endanger the damage to the hardware, and software of a ship, as well as loss of data. Hardware is the physical asset, and software and data are digital assets. For example, because the ECDIS of a new-build dry ship was infected by a virus, the ship was delayed from sailing for several days. The failure of the ECDIS appeared to be a technical disruption. A producer technician was required to troubleshoot, quarantine the virus, and

[19] Incident: Crash of integrated navigation at sea

restore the ECDIS computers. The delay in sailing and costs in repairs totalled hundreds of thousands of USD. Restoring the ECDIS systems include repairing or replacing equipment, computers, setting the navigation software, and restoring the data of the ship's navigation[20] (BIMCO, 2018).

In the case of a cyber risk causing physical contact such as collision, grounding, or contact with movable or fixed objects, the damages to the hull and machinery of the ship are inevitable.

- **Loss of cargo:** cyber risks may result in loss of cargo via sophisticated cyber fraudulent contrivances. Case study of the Iranian Shipping Line (IRISL) is a typical illustration. In 2011, hackers successfully accessed the company's servers, control business applications, and deliberately manipulated data embracing rates, loading information, cargo tracking numbers, and customer data. The containers were delivered to the wrong destinations and some of them were lost. IRISL's fleet and terminal operations were significantly impacted (North, 2017).
- **Personnel injury or death:** A cyber risk may lead to injury or death of seafarers or passengers, especially when it causes a severe accident like a collision with other ships or contact with fixed or movable objects.
- **Pollution loss and damage:** A cyber risk may result in discharge or escape of oil or any other substance into the sea especially when it causes a severe accident like a collision with other ships or contact with fixed or movable objects.

b. Loss or damage relating to company operation

- **Business interruption:** The severe impact of cyber risks on shipping companies is the disruption of business activities due to the shutting down of all of the informative, operative and administrative systems, which lead to significant financial losses such as loss of profit and cost of contract compensation.

[20] Incident: Unrecognised virus in an ECDIS delays sailing

- **Property damage:** Cyber risks could destroy the IT systems of the shipping company damaging both hardware and software, which would lead to the cost of repairing, replacing, restoring equipment, and programs. After a cyber attack, Maersk lost between USD 250-300 million to recover 49,000 endpoints (PCs, servers, and other networking apparatus) at 600 sites across 130 countries (BIMCO, 2019).
- **Cyber extortion:** Ransom is the financial loss, which the company has to pay in response to ransomware.
- **Financial loss due to wire transfer fraud:** The payments are transferred to the criminal's bank account by cyber fraud victims. In the maritime industry, these victims are not only shipowners but also charterers, agents, suppliers and crew manning agencies. With sophisticated techniques, great value payments are captured and unable to be recovered. In 2013, a fuel supply company, World Fuel Services (WFS) lost more than USD 1 million by cyber criminals, who installed spyware on the WFS computer network and created a fake email from WFS' supplier requesting wire transfer payment (Ship&Bunker, 2014).
- **Loss of data:** The data that could be stolen by cyber criminals are various. It could be the personal data of passengers in cruise ships including details of bank accounts and credit cards, cargo information, business and administrative data of Companies in the shipping industry, and crew information. In 2018, Austal - an Australia-based ferry and defense shipbuilder was attacked by hackers. The company's data management systems were stolen and some of them were offered for sale on dark website (Phish&Ships, 2017).
- **Regulatory penalties, fines, cost, and expenses:** Cyber risks could expose Companies to regulatory penalties and claims by an individual in terms of loss of personal data according to applicable law. In 2018, the General Data Protection Regulation (GDPR) of the EU came into force, which imposes penalties up to

Euro 20 million or 4 percent of a company's annual turnover for non-compliance with the GDPR[21].

- The consequences of cyber incidents also include crisis management costs and reputational impact that must be incurred by Company.

From the above analysis, it is conceivable that cyber-security risks in marine insurance intrinsically hold several features as follows:

- Maritime cyber-related risks are not excluded or restricted from the definition of "maritime perils" in the MIA 1906.
- Maritime cyber risks are not explicitly listed in the H&M and P&I insurance policies.
- Cyber risks could be a trigger causing other marine risks such as collision with other ships, grounding and stranding, accidents in cargo handling, contact with fixed and movable objects.
- Cyber risks could precisely be Inchmaree risks under IHC (1/11/03), in particular, the non-malicious actions of seafarers could be the negligence of the Master, officers or crew; malicious actions of seafarers could be the barratry of the Master, officers or crew; the weakness or vulnerability in ship's system could be a latent defect.
- The consequences caused by cyber risks relating to the ship operation could be loss, damage, cost, and expenses arising from the covered risks under the H&M and P&I insurance policies: property damage, personal injury or death, pollution loss and damage, and loss of cargo.

Actually, there is an exclusion in H&M insurance policy and ambiguity in P&I insurance policy in terms of liability of the insurer to loss and damage arising from cyber risks, which should be scrutinised in the next Chapter.

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR, 2016).

CHAPTER IV: LIABILITIES FOR LOSSES AND DAMAGES ARISING FROM CYBER-SECURITY RISKS

4.1 Liabilities in the Marine Insurance Act 1906

Article 55.1 of the MIA 1906 regulates a paramount principle, namely that the insurer is liable for the loss proximately caused by an insured peril, or in other words, the insurer is not liable for the loss, which is not proximately caused by an insured peril.

The assured must generally ascertain the proximate cause when he claims to recover a loss. The truly proximate cause is the real efficient cause of the loss and not necessarily the one which is nearest in time (Gurses, 2015). The efficiency of a proximate cause is judged as a dominant and decisive impact on and contribution to the loss. However, the determination of whether a cause is proximate or remote is complicated when numerous causes concurrently and simultaneously occur, especially in circumstances, where uninsured risks could be one of several causes of loss.

Article 55.2 of the MIA 1906 provides exclusions to the cover from a contract of marine insurance. Unless the policy otherwise provides, the insurer is not liable for any loss attributable to or proximately caused by:

- *The wilful misconduct of the assured (except the misconduct or negligence of the master or crew)*
- *Delay*
- *Ordinary wear and tear*
- *Ordinary leakage and breakage*
- *Inherent vice or nature of the insured property*
- *Rats or vermin*
- *Machinery injury which not proximate caused by maritime perils.*

Wordings “unless the policy otherwise provides” allows the particular insurance policies to provide other special exclusions. The H&M insurance policies normally preclude the risks of war and strikes, terrorists, political motives and malicious acts, radioactive contamination, chemical, biological, bio-chemical, and electromagnetic weapons. The P&I Clubs’ Rules generally exclude war risks, nuclear risks, the act of wilful misconduct, and other specific risks. Moreover, it is notable that the principle of “proximate clause” is also applied for excluded cover; however, it could be modified in particular policies due to the wording “unless the policy otherwise provides”.

Accordingly, it is necessary to determine the proximate cause(s) of a loss and if they are insured risks or uninsured risks according to marine insurance policies. In general, English law provides the principle where there are two proximate causes of loss under a claim, as follows:

(i) If one of which is specifically covered and the other is neither specifically covered nor specifically excluded, the claim would prevail;
(ii) If one of which is specifically covered and the other is specifically excluded, the claim would be failed (IUA, 2016).

The regulations of “proximate cause” and “included or excluded losses” in the MIA 1906 are critical principles of marine insurance law to determine the insurer’s liability. These principles are also legal ground concerning defining liabilities for the losses and damages arising from cyber risks. As mentioned in Chapter 3, cyber risks are not expressly regulated as maritime insured perils. In addition, the losses caused by cyber risks are not explicitly excluded in the MIA 1906. For a view on the practical approach, it is interesting to scrutinise the contemporary H&M policies and P&I Rules.

4.2 Liabilities in contemporary marine insurance policies

4.2.1 Hull and Machinery Insurance

In the marine insurance market, the H&M insurance policies are non-affirmative cyber exposure because they do not explicitly include or exclude losses that might occur via cyber risks. Particularly, the IHC (01/11/03) only declares the exclusions relating to war and strikes (Clause 29); terrorist, political motive and malicious acts (Clause 30); and radioactive contamination, chemical, biological, bio-chemical and electromagnetic weapons (Clause 31). As analysed in Chapter 3, cyber risks might trigger an insured peril; therefore, the H&M policy in doubt might cover cyber-related losses if the proximate cause of the loss is judged to be a peril insured against (Soyer, 2020).

Indeed, there are several exclusive or extensive clauses, which were introduced to the insurance market to deal with coverage of cyber risks as examined below:

a. Institute Cyber Attack Exclusion Clause (CL380 10/03)

Since 2003, the Institute Cyber Attack Exclusion Clause (CL380 10/03) has been added to H&M insurance policies to exclude the physical damage of vessels caused by a malicious cyber attack. Its essence is described by these wordings:

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

It certainly seems to be that the applicable scope of this clause is too broad with exclusions of both direct and indirect cyber-related causes. The below scenario might serve as an example[22].

Two vessels are insured by H&M insurances under IHC (01/11/03) incorporating CL380 (10/11/03) according to English law. Vessel A is navigating and uses ECDIS, which is updated via the internet while Vessel B is laid up in a recognised anchorage and complies with applicable lay-up requirements. Vessel A manoeuvres to the anchorage and collides with Vessel B. The investigation result illustrates that two weeks before the collision, the anchorage had been shown on the ECDIS chart; however, the update via the internet had deleted the anchorage data from the chart because of the malicious code. The officer on watch had not sailed in that area and had not been keeping a proper lookout. The investigator discovers the source of the malicious code as a cyber attack. There is no evidence to conclude the author of the malicious code is a terrorist or acting from a political motive.

Vessel A claims for damage to the vessel caused by a peril of the sea (collision) and the negligence of crew according to Clause 2.1.1 and 2.2.3 of the IHC (1/11/03). Vessel B claims for damage to the vessel caused by a peril of the sea (collision) under the Clause 2.1.1 of the IHC (1/11/03).

The key issues are the questions what was the proximate cause of the vessel's physical damages, and whether the insurers of Vessel A and Vessel B would be liable for the damages of these two vessels. Actually, the malicious code was the direct cause of the anchorage data deletion; however, it was not the direct cause of the vessel's damages. Because the deleted data, in this case, could not trigger a collision without the role of the officer of watch. The negligence of the officer of watch was the cause of the collision, and consequently, the collision resulted in the vessel's physical damages. The causation in this case was a chain, i.e. the first cause lead to the next ones. In addition, there is a direct nexus between the collision and the damages of the vessel, which proves that the collision is the proximate cause of the vessel's damages. The malicious code

[22] This scenario is modified from the Scenario - Marine Hull introduced by (IUA, 2016)

and negligence of the seafarer indirectly contributed to the vessel's damages; therefore, they are remote causes.

According to the IHC (1/11/03), the collision is an insured peril. In this case, the collision was the proximate cause; therefore, the insurer would be liable for the damages of the vessel. However, according to CL380, the malicious code is excluded risk. Although in this case, it was a remote cause, the assured would not recover the damages because the CL380 explicitly excludes damages indirectly caused by malicious code.

The other issue is the insurer needs to prove the malicious code that was used or operated as "a means of inflicting harm". Although there is no Court's decision or interpretation in the meaning of these words (Soyer, 2020), "inflicting" suggests a deliberate act and intention to cause "harm". It corresponds with the word "cyber attack" heading to the clause, whether on the targeted or untargeted victim. The malicious software or malicious code in the cyber security context might themselves be treated as a means of inflicting harm, especially if the source of malicious code is defined as an attacker instead of an innocent or benign actor.

It is concluded that any claim by Vessel A would be excluded by the terms of CL380; notwithstanding that, the collision or negligence of the crew has operated as an insured peril. Also, any claim by Vessel B would be precluded by CL380 or at least in an uncertain situation although Vessel B appears entirely innocent (IUA, 2016).

The CL380 is criticised by the insurance market because it is archaic and inappropriate to the demand of shipowners in protection property and transfer risks. Dating back to 2003, the insurers realised that the cyber threats existed; however, they could not have foreseen as well as evaluating the severity of cyber-related consequences today. With the heavy reliance on integrated technology of ship operation, from the bridge, machinery, communication to cargo handling systems, the wide scope of CL380 possibly counteracts the H&M insurance, especially if the insured property is an autonomous ship.

The cyber security experts are calling for revoking of the CL380 and implementing the applicable policies insuring against cyber risks (Sela, 2018). Indeed, the marine insurers have reviewed and offered the write-back or buy-back of this Clause. In

particular, the London marine insurance market released the **"CL380 Hull amended"** clause with explicit write-back of coverage for the traditional perils, which are triggered by or involved by cyber attacks (Cooper, 2019). The amendment includes the following term:

> *Where this clause is endorsed on policies covering marine risks, Clause 1.1 shall not operate to exclude loss or damage liability or expense (which would otherwise be covered) caused by:*
> *Perils of the sea, rivers, lakes or other navigable waters,*
> *Fire or explosion*
> *…*
> *Negligence of Master, Officer, Crew or Pilots …*
> *Nor, shall clause 1.1 operate to exclude the indemnity under the Collision Liability clause (which would otherwise be covered).*

Furthermore, the Norwegian Hull Club provides the **"Clause 380 buy-back"** covering for incidents that would otherwise not be recoverable due to CL380 exclusion (Norclub, 2020).

The amended clause and buy-back clause provide coverage for several traditional insured perils, which normally are the proximate causes of the loss while the cyber attacks mostly are remote causes. However, these proposals could not address whether the cyber risks might be covered as separate insured perils that proximately cause the ship's loss and damage. For instance, the ECDIS systems were infected by virus, and the cost in repairing and replacing the equipment, setting the software, restoring the data totalled in tens of thousands US dollars. Actually, this cost should be covered by the insurers, which could help the assureds to reduce their financial burden during managing and operating the vessel. In addition, although these products might address the wide scope of CL380, only the losses and damages arising from cyber attacks are recoverable whilst the cyber risks caused by non-malicious acts have not been taken into account.

b. LMA5402 - Marine Cyber Exclusion

In November 2019, Lloyd's Market Association produced new model clauses, which provide clarity about cyber coverage under first party property damages policies in the marine business, including LMA5402 - Marine Cyber Exclusion and LMA5403 – Marine Cyber Endorsement (LMA, 2019).

LMA5402 offers the market participants an option to exclude losses or damages at the widest application scope with the wordings as follows:

This clause shall be paramount and shall override anything in this insurance inconsistent therewith.

1 In no case shall this insurance cover any loss, damage, liability or expense directly or indirectly caused by, contributed to by or arising from:

1.1 the failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system, or

1.2 the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

This clause clearly and explicitly excludes the loss or damages directly or indirectly caused by, contributing to or arising from the use or operation of a computer system not only as a means for inflicting harm but also as a failure, error or malfunction resulting in the non-malicious actions or the inherent weakness of the system. It is clear that the drafters have taken into account the most prominent sources of cyber risks and resolved the ambiguities of the "silent cyber" or "non-affirmative cyber exposures" policies at the attitude of excluding cyber cover.

c. LMA5403 - Marine Cyber Endorsement

LMA5403 offers another option that enables participants to exclude cyber-related loss in circumstances where the computer system is used or operated to inflict harm and only provides cover in circumstances where the computer system is NOT used or operated to inflict harm. A new term is introduced as follows:

> *2. Subject to the conditions, limitations and exclusions of the policy to which this clause attaches, the indemnity otherwise recoverable hereunder shall not be prejudiced by the use or operation of any computer, computer system, computer software programme, computer process or any other electronic system, if such use or operation is not as a means for inflicting harm.*

This endorsement provides the obvious stance of insurers relating to exclusive or affirmative cyber coverage. Marine insurers continue to be prudent when they only insure against cyber risks caused by the non-malicious actions or the inherent weakness of the system. The loss and damage arising from the malicious actions such as cyber attack are continuously precluded. It might be explained that marine insurers still believe a ship being able to manoeuvre or anchor by traditional means even if the cyber risks occur (LMA-JHC, 2016). Nonetheless, the issuance of LMA5402 and LMA5403 is currently the starting point for the market to address cyber risks in response to aggressive and increasing cyber threats in the maritime industry.

4.2.2 Protection and Indemnity Insurance

In 2018, a survey conducted by Fairplay, BIMCO, and ABS reported that out of 16% of cyber incidents covered by insurance, there are two-thirds of the claims used specific cyber policy, while one-third of the claims used P&I insurance (Fairplay, BIMCO, ABS, 2018). At present, 13 Clubs providing P&I insurance are members of the International Group of P&I Clubs (IG), where more than 90% of the shipowners of the

world are entered. To recognize the cyber coverage under the P&I insurance, this Chapter will review the Rules 2020-2021 of 13 Clubs, who are the American Club, Britannia P&I, Gard, Japan P&I Club, the London P&I Club, North, Shipowners' Club, Skuld, Standard Club, Steamship Mutual, the Swedish Club, UK P&I, and West.

In general, 13 Clubs' Rules have no expressly specific exclusion of cyber risks other than several special circumstances; however, these Rules also have no explicit affirmation of cyber risk coverage. Indeed, if a ship is compromised by cyber risks leading to the shipowner's liability to third party, which falls within P&I cover, the shipowner could claim for P&I liability, such as collision, personal injury, property damage, pollution, wreck removal, or fines. For example, an onboard LAN system of a ship was infected by a virus via email, which caused the electronic aid for navigation and propulsion to break down. At the time of departure, the ship collided with the harbour facilities leading to the shipowner's liability for the harbour facilities damage (JPC, 2018). Nonetheless, there are several special exclusions relating to cyber elements in Clubs' Rules as analysed below.

a. Electronic trading system

13 P&I Clubs exclude any liabilities, losses, costs, and expenses arising from the use of any electronic trading system, which is any system replaces or is intended to replace paper documents used for the sale of goods and/or carriage by sea and other means of transport[23], for example, the use of electronic bills. The principal reason is the legal uncertainty that there are currently no international conventions or laws regulating the use of electronic bills (Gard, 2013). Although the Rotterdam Rules allow the electronic transport documents to be used and to have the same effect as traditional paper bills; however, this convention has not yet entered into force. Another reason is the vulnerability of the electronic trading system which is effortlessly compromised by cyber risks.

The case of ***MSC Mediterranean Shipping Co SA v. Glencore International AG*** is a typical example. Three containers were to be delivered via Electronic Release

[23] Gard's Rules 2020, Rule 63 (j) Excluded losses, (see Appendix 2)

System (ERS), which the discharge port (Antwerp Port) had introduced in 2011, and the Carrier MSC and Shipper Glencore had used in the previous 69 successful cargo deliveries. At the 70th carriage of three containers from Fremantle to Antwerp, when the Glencore's agency lodged with MSC one of the bills of lading, MSC sent a release note and PIN code to Glencore's agency for delivery of cargo via the ERS. However, the PIN code was hacked resulting in two containers being stolen by unauthorised recipients (SSM, 2017). The ERS is a type of electronic trading system, which entitle the holder of electronically generated information/document to delivery or possession of the cargo. MSC would be liable for the lost containers; however, the P&I insurer would not cover the loss of cargo due to the paperless trading exclusion being triggered.

b. War risks

Besides paperless trading, 13 Clubs expressly exclude war risks from the scope of their cover. Therefore, when the cyber risks fall into the definition of war risks under the P&I Clubs' Rules, they will not normally be insured. Generally, the P&I Clubs' Rules provide that:

> *The Association shall not cover under a P&I entry liabilities, losses, costs or expenses (…) was caused by:*
>
> *a) war, civil war, revolution, rebellion, insurrection or civil strife arising therefrom, or any hostile act by or against a belligerent power or any act of terrorism (…);*
>
> *b) capture, seizure, arrest, restraint or detainment, (barratry and piracy excepted), and the consequences thereof or any attempt thereat;*
>
> *c) mines, torpedoes, bombs, rockets, shells, explosives, or other similar weapons of war (…)*[24]

[24] Gard Rules 2020, Rule 53 War Risks, (see Appendix 2)

Under the war risk exclusion clause, it is worth stressing that any act of terrorism is commonly excluded from P&I cover. The insurer has the right to decide whether or not an act constitutes an act of terrorism. In fact, several reports show that many cyber attacks are derived from political motivation and thus this could be very unfavourable for shipowners to recovery the loss and damage under P&I policies (Soyer, 2020).

If responding to the exclusion of war risks under the standard P&I Rules, the shipowners normally take out the war risk extension clause as an additional insurance. The P&I insurance shall cover the liabilities, losses, costs, or expenses caused by war risks with special terms negotiated between the insurers and assureds. However, even if under the special war risk coverage, the insurers shall not be liable for any liabilities, losses, costs, or expenses directly or indirectly caused by, contributed to by, or arising from the use or operation, as a means for inflicting harm, of any computer virus[25]. There are eight Clubs[26] that expressly regulate this exclusion under their Rules.

In addition, relating to the war risk extension clause, the cover of P&I insurance is extended to include the liability of assureds:

(i) to pay damage, compensation or expenses in consequence of crew injury, illness, or death (including deviation, repatriation and substitute expenses and shipwreck unemployment indemnity);

(ii) *legal costs and expenses incurred solely for the purpose of avoiding or minimizing any liability or risk insured by P&I Club.*

where such liability directly or indirectly arising from the use or operation as a means for inflicting harm, of any computer, computer system, computer software

[25] Gard Rules 2020, Appendix I, Additional Insurances, Rule 2 War risks, Sub title Bio chem and computer virus, Clause 4 (ii), (See Appendix 3).
[26] They are Gard, Japan P&I Club, North, Shipowners' Club, Skuld, Standard Club, Steamship Mutual, and West.

programme, malicious code or virus or process, or any electronic system[27]. The limitation of liability shall be in aggregate USD 30 million per ship. Losses caused by the use of the ship or its cargo to inflict harm, or the use of computer, computer system or computer software program to launch, guide or fire a weapon or missile would be excluded[28]. There are seven P&I Clubs[29] providing this special cover.

c. Maritime Labour Convention Extension Clause

P&I Clubs provide the MLC Extension Clause to discharge and pay on the assured's behalf liabilities in respect of outstanding wages, repatriation cost and expenses, compensation for death or long-term disability of seafarers according to MLC 2006. However, there are nine Clubs[30] that shall not cover these liabilities as they are directly or indirectly caused by, or contributed to by, or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, computer virus or process, or any other electronic system[31].

In summary, the uncertainty of P&I Rules relating to affirmative or non-affirmative cyber exposure might lead to insurance gaps in determining whether a claim falls within or outside P&I cover. For example, the information system of a cruise vessel was infected by a virus. The credit card information of passengers was hacked and a huge amount of money was illegally withdrawn from the banks resulting in the passengers' financial losses. The question is whether the P&I insurance covers the liability for the financial losses of passengers or not. The ambiguity is demonstrated that shipowners are normally aware that the data loss will be covered by non-marine insurance (BIMCO, 2018), and the definition of "personal property" in P&I Clubs' Rules does not included intangible

---

[27] Gard Rules 2020, Appendix I, Additional Insurances, Rule 2 War risks, Sub title Bio-chem and computer virus clause, (see Appendix 3).
[28] Gard Rules 2020, Appendix I, Additional Insurances, Rule 2 War risks, Sub title Bio-chem and computer virus clause, (see Appendix 3).
[29] They are Gard, Japan P&I Club, Shipowners' Club, Skuld, Standard Club, Steamship Mutual, West.
[30] They are the American Club, Gard, Japan P&I Club, Shipowners' Club, Standard Club, Steamship Mutual, the Swedish Club, UK P&I, West.
[31] Gard Rules 2020, Appendix IV Passengers and Seamen, Clause 4 Maritime Labour Convention Extension Clause 2016, (see Appendix 4).

assets as personal data. However, the liability for passenger's financial loss in this case obviously is a kind of third party's liability, and the loss of data also occurs from the cruise ship's operation. Even if the Steamship Mutual P&I Club has released the guidance on the EU's GDPR to their Members and recommended that "*the impact of this regulation will most often be felt in claims relating to personal injury and illness or other cases involving data originating from natural personal, or individuals*" (SSM, 2018).

In addition, in the event of claims falling into the P&I coverage, the arguments between insurers and assured could happen in many circumstances. A case in point is if the vessel's navigation systems were infected by a virus via the seafarer's USB stick resulting in collision and seafarers' injury. The P&I insurance would cover as usual; however, this claim could be failed due to the argument of inadequate cyber security training implemented by the assured (Souli, 2020).

Besides, the ambiguity also manifests what kinds of cyber risks might be insured under P&I Rules, whether malicious actions, non-malicious actions or the inherent weakness of the ship's system. This is the reason experts recommend that Companies should seek the consultation with insurers or brokers on recoverable cyber risks before signing insurance contracts (BIMCO, 2018).

4.3 Standalone Cyber Clause

The traditional marine insurances expose the coverage gaps where cyber risks are concerned. To narrow these gaps, besides the buy-back or write-back offers of cyber attack clauses, the Lloyd's insurance market has recently introduced a standalone cyber insurance product, which covers the losses and damages of the First Party and Third Party as follows (Marine Cyber Insurance, 2020):

a. First Party:

- Maritime cyber response costs embrace the reasonable and necessary costs and expenses to engage a lawyer, appoint a public relation consultant, and forensic costs;

- Maritime IT system restoration costs cover the direct damage to the data or programs up to the Limit of Liability;
- Insured's Network Failure - Income loss and extra expense which are insured against the business interruption directly caused by any of the items listed during the Period of Restoration;
- Cyber extortion and ransomware;
- Cyber crime over for electronic wire transfer fraud.

b. **Third Party:** Covers liability for third party in respect of losses resulting from breaching the network security and private or confidential information.

c. **Other liability:** The standalone cyber insurance clause offers the cyber attack CL380 buy-back and customer cargo damage/deterioration mitigation clauses.

With these insured liabilities, it seems likely that the physical damage of the vessel and the liability of the shipowner to the third parties concerning the vessel's operation are not addressed by the standalone cyber clause. This product is likely preferred to protect the assured in respect of Company operation rather than vessel operation.

Based on the above analysis, it is therefore worth summarising that the marine insurers are struggling to determine the liability for losses and damages arising from cyber-security risks. The H&M insurance with integrated CL380, the P&I insurance, and the Standalone Cyber Clause could not provide a comprehensive cyber risk coverage. Therefore, establishing a special marine cyber-security risk clause that insures against the cyber risks on ship systems is indispensable. It should be an extension clause incorporating the H&M and P&I policies like the format of the War Risk Extension Clause. In addition, there are several articles in terms of cyber elements under H&M insurance policies and P&I Clubs' Rules, which should be considered to revise. The suggested resolution will be discussed in Chapter V.

CHAPTER V: RECOMMENDED STANDARD CYBER-SECURITY RISK CLAUSE IN MARINE INSURANCE

5.1 Standard cyber-security risk clause

From the understanding of cyber risk nature and the current situation of cyber-related liabilities under traditional insurance products as well as the specific standalone cyber risk insurance. This clause is drafted by the author of this dissertation with the ambition to design a product of comprehensive cyber risk cover, which could be applied for ship operations. The drafting is based on the research of cyber-security risks and liabilities, the approach of cyber risk management of IMO and industrial guidelines, in comparison with the exiting cyber risk clauses introduced to market such as CL380 Hull amended, LMA5402, LMA5403, and standalone cyber clause as analysed in previous Chapters. The wording of this suggested clause is introduced as follows:

Cyber Risk Extension Clause

1. Subject to the conditions, limitations, and exclusions of the policy to which this clause attaches, this insurance shall cover loss, damage, liability, or expense caused by, or contributed to by, or arising from malicious action(s) which present cyber risks including:
   (i) unauthorised access, manipulation, or disruption of the IT and/or OT system of a ship;
   (ii) any failure or loss of availability or integrity of the IT and/or OT system of a ship;
   (iii) any loss of availability, integrity, or confidentiality of information and data of a ship.

2. Subject to the conditions, limitations, and exclusions of the policy to which this clause attaches, this insurance shall cover loss, damage, liability, or expense caused by, or contributed to by, or arising from non-malicious action(s) which present cyber risks including:
   (i) unauthorised access, manipulation, or disruption of the IT and/or OT system of a ship;
   (ii) any failure or loss of availability or integrity of the IT and/or OT system of a ship;
   (iii) any loss of availability, integrity, or confidentiality of information and data of a ship.
3. Notwithstanding the paragraph 1 and 2 above, in no case shall this insurance cover loss, damage, liability or expense directly or indirectly caused by, or contributed to by, or arising from any failure or weakness in design, construction and/or maintenance of IT and/or OT system of a ship (except any latent defect of IT and/or OT system), provided that there is no any occurrence or impact of malicious action(s) or non-malicious action(s) on that loss, damage, liability or expense.

Definitions

4. **Malicious actions:** are deliberately wrongful acts presenting cyber risks and committed by any individual(s) or organization(s) whether externally or internally involved in ship operation that result in loss, damage, liability, or expense to the ship.
5. **Non-malicious actions:** are unwitting acts presenting cyber risks and committed by any individual(s) or organization(s) whether externally or internally involved in ship operation that result in loss, damage, liability, or expense to ship.
6. **IT system:** any hardware, software, communication technologies, and associated networking that manages/controls the data and information processing.

7. **OT system:** any hardware, software, communication technologies, and associated networking that directly monitors/controls physical devices and processes onboard ships.

This new clause is designed to cover the cyber risks arising from malicious actions and non-malicious actions. While the other insurance clauses, such as CL380, P&I rules, LMA5402, LMA5403 normally draft the wording "*use computer as a means for inflicting harm*" or "*use of computer is not as a means for inflicting harm*" to express and distinguish the nature of cyber risks. However, this expression could not reflect motives of actors triggering cyber risks, which are intentional or unintentional. Because after all, triggering cyber risks whether intentionally or unintentionally, is harmful for an insured subject. This is the first time the terms "malicious actions" and "non-malicious actions" are being introduced in a cyber risk extension clause as a unique classification.

In addition, the ship's non-compliance in relation to design integration and maintenance of the IT and/or OT system should not be covered. The principal reason is the insurers need to exclude any risks, which are not accidental and unforeseen act or event as well as being actively controlled or avoided by the assureds.

To implement this extension Clause, the term "ship" in the MIA 1906 Schedule 1, Rule 15 should be considered to be revised. The existing wording is:

> *The term "ship" includes the hull, materials and outfit, stores and provisions for the officers and crew, and, in the case of vessels engaged in a special trade, the ordinary fittings requisite for the trade, and also, in the case of a steamship, the machinery, boilers, and coals and engine stores, if owned by the assured.*

Obviously, according to this term, the ship only includes the tangible properties. The intangible properties, such as computer software, computer programme, and ship's data will not be considered as a part of the ship's property. It means that the loss of or damage to computer software, computer programme, and ship's data could not be

considered as physical damage and covered by insurers. This issue might be prejudiced to shipowners because the cost of software, programme, and ship's data had been contributed to the ship's price and had been added to the insured value. Therefore, the MIA 1906 should revise the term of "ship", in which the computer software, computer programme, and ship's data should be considered as a part of the ship i.e. a part of the insured property. However, it is not easy to expeditiously amend the MIA 1906 when the first amendment with the most significant changes for over 100 years were made by the Insurance Act 2015. Probably, the marine insurance market should address this issue by insurance contracts, policies or special negotiation between insurers and assureds.

5.2 Recommendations for Hull and Machinery Insurance

The marine insurers should withdraw the CL380 from H&M insurance policies. In the short term, it may be problematic as insurers depend on the reinsurance terms, which also incorporate CL380. However, there are several rational reasons to revoke this controversial Clause. Firstly, with a high and increasing probability of cyber attacks to a ship with various methods today, an 18-year-old Clause that excludes the loss and damage to computer systems, or software programmes is archaic. It could not keep up with the change of technology and could not meet the requirement of shipowners in demand to transfer the new risks. Secondly, the wide application scope of CL 380 leads to the coverage gap of H&M insurance policies, which is the greatest weakness of this conventional insurance line. Thirdly, CL380 may be detrimental to the assureds in circumstances that the loss is triggered by two proximate causes, in which one is an insured peril whilst another is an excluded risk, so the loss will be not covered by insurers according to the principle of English law.

5.3 Recommendations for Protection and Indemnity Insurance

With the Cyber Risk Extension Clause integrated into the P&I Rule, the ambiguity of cyber coverage will be clarified. It also clearly distinguishes which types of cyber risks should be insured against. P&I insurance continuously fulfils the mission to protect shipowners against their liabilities for loss of life and personal injury as well as the loss

and damage arising from the cyber risks, which are not covered by H&M policies. To be consistent with this Clause, there are several terms in P&I Clubs' Rules, which should be considered to be revised as follows:

Firstly, the liabilities, costs, or expenses arising from the use of any electronic trading system should not be excluded by P&I insurance. Actually, the greatest numbers of claims experienced by a P&I Club are cargo claims (Gurses, Hjalmarsson, & Pilley, Marine Insurance, 2014). Meanwhile, electronic documents have been used by the major container carriers over forty years despite the legal uncertainty (Martin-Clark, 2010). This demand may continuously rise due to the serious disadvantages of paper bills of lading such as the loss of time and high possibility to produce the forged or counterfeit ones.In addition, the electronic trading system also faces the cyber risks as mentioned in Chapter 4. Therefore, the liability of the carrier for loss or damage of cargo arising from paperless trading would be considerable and increasing, which needs to be covered by the P&I insurers.

Secondly, under the war risk extension clause, the P&I Clubs should delete the regulation in terms of the insurers shall not be liable for any losses caused by any computer virus as a means for inflicting harm. Currently, this regulation reveals the P&I Clubs' stance of absolute avoidance to cyber risks as the cyber exclusion states in the extension clause. However, when the P&I insurers' attitude changes by incorporating the Cyber Risk Extension Clause into the Rules, the computer virus exclusion should be removed from the war risk extension clause.

Thirdly, under the Maritime Labour Convention Extension Clause, the exclusion of liabilities for several seafarers' benefits and compensation caused by the use or operation of computer system, software, or computer virus as a means for inflicting harm should be removed. Although when drafting this term, the underwriters assumed that, a ship being lost due to cyber attack is inconceivable (BIMCO, 2019). However, this position should be changed when the cyber risks are explicitly covered by P&I insurance. This will contribute to enhancing the effectiveness of the Maritime Labour Convention 2016 to protect the legal rights and benefits of seafarers.

Fourthly, the definition of “personal effects” or “personal property” should include personal data or personal information. It could protect the interest of crew, passengers, and onboard persons other than crew or passengers from the loss of data caused by cyber risks.

5.4 Implementation of Cyber Risk Extension Clause

With the comprehensive scope of coverage of the Cyber Risk Extension Clause as suggested above, the insurance companies obviously will face a number of claims and large pay-outs of indemnity. To reduce their exposure to financial risks, this Clause should be offered to cyber resilient ships and the shipowners have to implement an adequate cyber risk management.

To meet these compulsory conditions, the assureds must exercise due diligence to make the insured ship seaworthy. According to section 39.4 of MIA 1906, the “seaworthiness” requires the ship to be “*reasonably fit in all respects to encounter the ordinary perils of the seas of the adventure insured*”. The connotation of reasonable fitness in all respects is the safety of ship extending to construction, equipment, crew manning, adequate freeboard, and other safety requirements and procedures (Mukherjee & Brownrigg, 2013). The “reasonable fitness” is also the safety in carriage of contractual goods or other moveables to the destination as stated in section 40.2 of MIA 1906. In voyage policies, there is an implied warranty of ship’s seaworthiness that the assured has a duty to exercise at the commencement of the voyage and at all different stages of the voyage. In time policy, there is no implied warranty of seaworthiness; however, the assured (with the privity) shall not send the ship to sea in an unseaworthy status. Breaching the obligation of warranty could lead to the lawful refusal to indemnify the assured for the loss and damage.

In particular, the IHC (01/11/03) regulates the seaworthiness of the ship in Clause 13 - Classification and ISM, and Clause 14 - Management. Therefore, the assured has the duty to comply with all statutory requirements of the vessel’s flag state relating to construction, adaptation, condition, fitment, equipment, operation and manning of the

vessel[32]. The assured shall maintain the valid DOC and insured vessel's SMC as required by the ISM Code and Chapter IX of the SOLAS 1974[33].

As mentioned in Chapter 2 above, the cyber risk management is encouraged to be addressed in the SMS from 1 January 2021 on the basis of reference to flag state's requirements as well as international and industrial standards and best practice. It should be acknowledged that many flag states have issued the regulations to implement IMO guidelines as the mandatory requirements to deal with cyber risks in safe and secure shipping operations. It means that after 1 January 2021, the cyber risk management will be verified under internal audit and ship-based survey procedures. Therefore, any deficiencies or non-compliances could demonstrate the assured lacks adequate cyber security, which could potentially lead to an insured ship to be found unseaworthy, and consequently, insurance claims could be failed.

Accordingly, the prerequisite to apply the Cyber Risk Extension Clause is that the cyber risk management must be mandatorily implemented as a part of SMS and certified by the valid DOC of the assured and SMC of the insured vessel. However, the IMO's instruments relating to cyber risk management are currently non-mandatory without any sanctions. The compliance and implementation of IMO guidelines depend on the self-commitment of the rules-compliant and well-performing flag state (Daum, 2019). This legal uncertainty is the most significant barrier to the marine insurer offering the Cyber Risk Extension Clause as a marine cyber insurance product to the market. The maritime stakeholders should continue to foster the progress of adopting the internationally mandatory regulations in terms of cyber security in the maritime industry. They are the principal legal grounds to promote marine cyber risk insurance.

[32] Clause 14.4.1 IHC (1/11/03)
[33] Clause 13.1.4 and Clause 13.1.5 (1/11/03)

CHAPTER VI: SUMMARY AND CONCLUSION

In summary, with analyses and illustrations in this dissertation, it is widely recognized that cyber risks are inevitable dangers and could cause tremendous losses and damages to the maritime industry. Nevertheless, the marine insurers are starting to be aware of the market demand and prudently affirm the cyber coverage with extremely limited extension under the conventional marine insurance lines. This could not meet the shipowners' demand relating to cyber risk transfer. Furthermore, the standalone cyber insurance clause could not address the cyber-related losses and damages of the ship's hull and machine as well as the shipowner's liabilities to the third party incurred during the process of ship's management and operation.

The Cyber Risk Extension Clause suggested in this dissertation provides more comprehensive cyber coverage, which could be integrated - as an additional insurance clause - into both H&M and P&I insurances. It could address the complication of cyber risk nature in the maritime domain, corresponding to the approach and expectation of the Prudential Regulation Authority (PRA) expressed in the Letter on 30 January 2019 with title **"Cyber underwriting risk: follow-up survey results"** and Lloyd's announcement on 4 July 2019 with the tittle **"Providing clarity for Lloyd's customer on coverage for cyber exposures"**. PRA expected insurers to manage and reduce the unintended exposure, which can be caused by non-affirmative cyber risks (PRA, 2019). Lloyd's called for insurers to ensure all policies affirm or exclude cyber cover before 1 January 2020 and recommended to "*define cyber risk as any risk where the losses are cyber-related, arising from either malicious acts (e.g. cyber-attack, infection of an IT system with malicious code) or non-malicious acts (e.g. loss of data, accidental acts or omissions) involving either tangible or intangible assets*" (Lloyd's, 2019).

With this additional Clause, the assureds could effectively utilise the conventional insurances to cover modern risks. They could also reduce the insurance cost of purchasing both traditional insurance policies and standalone cyber risk products, which still inadequately cover the cyber risks relating to ship operation. With this additional Clause, the assureds could effectively utilise the conventional insurances to cover modern risks. They could also reduce the insurance cost of purchasing both traditional insurance policies and standalone cyber risk products, which still inadequately cover the cyber risks relating to ship operation.

The MIA 1906 with open regulations in terms of insured risks as well as included and excluded losses could give the insurers the opportunity to supplement cyber risks as the insured perils to conventional marine insurance policies. Accordingly, the Cyber Risk Extension Clause will not have a legal obstacle to be issued and applied in practice. However, the marine insurers and maritime insurance law makers should consider broadening the connotation of the term “ship”, which should include computer software, computer program, and ship’s data as intangible assets. In addition, the wordings of contemporary H&M policies and P&I Clubs’ Rules should be reviewed and revised to be consistent with the new cyber extension coverage.

The maritime industry is driving the great movement towards mitigating the threats from cyber risks. The IMO instruments, industrial guidelines on marine cyber security established a milestone of paradigm change of safety and security in shipping, charter parties, carriage of goods by sea, and marine insurance. The lack of adequate cyber security will affect the concept seaworthiness of a vessel, which results in numerous legal consequences to marine stakeholders not only fines and detentions but also contractual disputes. Marine insurance is an effective instrument to transfer cyber risks; therefore, the clarity of cyber affirmative or non-affirmative exposure is also a significant change of the marine insurance market (for both insurers and reinsurers) to be consistent in the cyber risks approach of IMO instruments and industrial guidelines.

Above all, the marine cyber insurance product needs the certainty of legal ground and effective implementation of cyber risk management, which maritime stakeholders embracing law and policy makers, courts, maritime authorities, classification societies,

marine insurers, shipowners, contractual parties, and seafarers should continuously establish and improve.

References

I. Legal documents, IMO's instruments, and industrial guidelines

BIMCO. (2018). *The Guideline on cyber security onboard ships version 3*. Retrieved from BIMCO: https://www.bimco.org/ships-ports-and-voyage-planning/security/cyber_security/cyber-security-guidance

IACS. (2020, April). *Recommendation on Cyber Resilience No.166.* Retrieved from International Association of Classification Societies: www.iacs.org.uk

ISM Code. (1998, July 1). Retrieved from International Maritime Organization : http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx

ISPS Code. (2004, July 01). Retrieved from International Maritime Organization : http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

GDPR. (2016, April 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.* Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

MIA. (1906). *Marine Insurance Act 1906*. Retrieved from UK Legislation : https://www.legislation.gov.uk/

MSC.428 (98). (2017, June 16). *Maritime Cyber Risk Management in Safety Management Systems* . Retrieved from International Maritime Organization,: https://docs.imo.org/Search.aspx?keywords=MSC%2098%2F23%2FAdd.1

MSC101/4/4. (2019, April 09). *MSC 101/4/4 - Measures to enhance maritime security.* Retrieved from International Maritime Organisation IMODOCS: https://docs.imo.org/Search.aspx?keywords=MSC%20101%2F4%2F4

MSC-FAL.1/Cir.3. (2017, July 5). *Guidelines on Maritime Cyber Risk Management.* Retrieved from International Maritime Organzation - IMODOCS: https://docs.imo.org/Search.aspx?keywords=MSC-FAL.1%2FCirc.3

II. Books

Cooper, S. (2019). Cyber risk, liabilities and insurance in the maritime sector. In B. Soyer, & A. Tettenborn, *Maritime liabilities in a global and regional context* (pp. 103-117). New York: Informa Law from Routledge.

Donner, P. (2016). *Commercial Law and Marine Insurance Text Book.* World Maritime University.

Gurses, O. (2015). *Marine Insurance Law.* Oxon & New York: Routledge.

Gurses, O., Hjalmarsson, J., & Pilley, R. (2014). Marine Insurance. In Y. Baatz, *Maritime Law.* New York: Informa Law from Routledge.

Martin-Clark, D. (2010). Electronic documents and the Rotterdam Rules. In D. Thomas, *The carriage of goods by sea under the Rotterdam Rules* (p. 283). London : Lloyd's List Law.

Mukherjee, P. K., & Brownrigg, M. (2013). *Farthing on International Shipping.* Verlag Berlin Heidelberg: Springer.

Rose, F. D. (2012). *Marine insurance law and practice.* London: Informa Law.

Soyer, B. (2020). Cyber risks insurance in the maritime sector: growing pains and legal problems. In P. K. Mukherjee, M. Q. Mejia, & J. Xu, *Maritime Law in Motion, WMU Studies in Maritime Affairs, Volume 8* (pp. 672-641). Springer Nature Swizeland AG .

Thomas, D. R. (2009). The concept and measure of indemnity in marine policies. In D. R. Thomas, *The modern law of marine insurance Volume 3* (p. 11). London: Informa Law Moritimer House.

III. Articles, reports and other materials

AGPS. (2019). *Allianz Risk Barometer top business risks for 2019.* Retrieved from Allianz Global Corporate & Specialty: https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2019.html

Baker, J. (2020, April 15). *MSC shutdown throws spotlight on cyber security*. Retrieved from Lloyd's List: https://lloydslist.maritimeintelligence.informa.com/LL1131940/MSC-shutdown-throws-spotlight-on-cyber-security

BIMCO. (2019). *Saety at sea and BIMCO cyber security white paper.* Retrieved from IHS Markit: https://cdn.ihsmarkit.com/www/pdf/1019/Safety-at-Sea-and-bimco-cyber-security-white-paper.pdf

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of cyber policy* , Vol.2, No.1, 53-63.

CyRiM. (2019). *CyRiM Report 2019 - Shen attack Cyber risk in Asia Pacific ports.* Retrieved from Lloyd's : https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/shen-attack-cyber-risk-in-asia-pacific-ports

Daum, O. (2019). Cyber security in maritime sector . *Journal of Maritime Law and Commerce* , Vol.50, No.1.

DG. (2019, November 7). *Cyber security and threats November 2019 week one - Vessel impersonation report* . Retrieved from Dryad Global : https://dryadglobal.com/cyber-security-threats-november-2019-week-one/

DNV-GL. (2016, September). *Recommended Practice - Cyber security resilience management for ships and mobile offshore units in operation.* Retrieved from DNV-GL: https://www.dnvgl.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html

Fairplay, BIMCO, ABS. (2018, August). *Maritime Cyber Survey 2018 - the results.* Retrieved from BIMCO: https://www.bimco.org/news/priority-news/20180924-cyber-security-survey

Gard. (2013, April). *Gard Guidance on Maritime Claims and Insurance* . Retrieved from Gard P&I Club: http://www.gard.no/Content/20823111/Gard%20Guidance%20on%20Maritime%20Claims_final.pdf

HFW. (2016). *Cyber Pack.* Retrieved from Cybersail: https://cybersail.org/wp-content/uploads/2017/02/HFW-Cyber-Pack.pdf

IACS. (2020, May 4). *IACS launches single standalone recommendation on cyber resilience.* Retrieved from International Association of Classification Societies : http://www.iacs.org.uk/news/iacs-launches-single-standalone-recommendation-on-cyber-resilience/

IFoA. (2019). *Silent Cyber Assessment Framework* . Retrieved from Institute and Faculty of Actuaries: https://www.actuaries.org.uk/system/files/field/document/FINAL%20Sessional%20paper%20-%20Silent%20Cyber%20Assessment%20Framework_0.pdf

IGP&I. (2019). *Group Agreements.* Retrieved from International Groups of P&I Clubs : https://www.igpandi.org/group-agreements

Insurance Marine News. (2020, June 18). Retrieved from Surge in maritime cyber-attacks reported: https://insurancemarinenews.com/insurance-marine-news/surge-in-maritime-cyber-attacks-reported/

IUA. (2016, January). *Cyber risk and insurance - An introduce to cross class cyber liabilities* . Retrieved from Maritime London : https://www.maritimelondon.com/wp-content/uploads/2016/01/005_Cyber_Risks_Combined_110116.pdf

JPC. (2018, May). *Cyber risk and cyber security countermeasures - P&I Loss Prevention Bulletin, Vol 42*. Retrieved from Japan P&I Club: https://www.piclub.or.jp/wp-content/uploads/2018/05/Loss-Prevention-Bulletin-Vol.42-Full.pdf

Knowler, G. (2017, August 16). *Maersk back in black in Q2, but warns of USD300 million cyber attack losses*. Retrieved from Safety at Sea : https://safetyatsea.net/news/2017/maersk-back-in-black-in-q2-but-warns-of-usd300-million-cyber-attack-losses/

Ladbury, A. (2020, March). *Partnership needed to tackle cyber threat to maritime sector* . Retrieved from The Marine Insurer: https://marineinsurer.co.uk/the-marine-insurer/

Lloyd's. (2019, July 7). *Market Bulletin Ref: Y5258*. Retrieved from Lloyd's : https://www.lloyds.com/~/media/files/the-market/communications/market-bulletins/2019/07/y5258.pdf

LMA. (2019, November 13). *Lloyd's Market Association Bulletin - Property and Marine Cyber Clauses* . Retrieved from Lloyd's Market Association: https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA19-031-PD.aspx

LMA-JHC. (2016, September 12). *Hull Insurance and Cyber* . Retrieved from Lloyd's Market Association: https://www.lmalloyds.com/LMA/Underwriting/Marine/JHC/jhc_circulars.aspx

Maersk. (2017). *Cyber attack update announcement*. Retrieved from http://investor.maersk.com/news-releases/news-release-details/cyber-attack-update

Marine Cyber Insurance. (2020). Retrieved from Marine Cyber Insurance: https://www.maritimecyberadvisors.com/cyber-insurance/

Norclub. (2020). *Cyber Clause 380 buy-back*. Retrieved from Norwegian Hull Club : https://www.norclub.com/products/special-risks/cyber-clause-380-buy-back-/

North. (2017, July). *Loss prevent briefing - Cyber risk in shipping.* Retrieved from The North of England P&I Association : https://maritimecyberadvisors.com/_files/200000061-b1372b2348/Cyber-Risks-in-Shipping-LP-Briefing.PDF

Phish&Ships. (2017, July). *Key takeaways from recent cyber attacks in shipping, Phish&Ships No.32*. Retrieved from Safety4sea: https://safety4sea.com/wp-content/uploads/2019/07/Be-Cyber-Aware-at-Sea-Phish-and-Ships-2019_07.pdf

PRA. (2019, January 30). *Cyber underwriting risk: follow-up survey results*. Retrieved from Bank of England - Prudential Regulation Authority : https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2019/cyber-underwriting-risk-follow-up-survey-results

Sela, I. (2018, September 19). *Naval Dome calls on Insurers to revoke Clause CL380*. Retrieved from The Maritime Executive : https://www.maritime-executive.com/corporate/naval-dome-calls-on-insurers-to-revoke-clause-cl-380

Ship&Bunker. (2014, October 13). *Recent cyber attacks highlight bunker industry vulnerability* . Retrieved from Ship&Bunker: https://shipandbunker.com/news/am/171559-recent-cyber-attacks-highlight-bunker-industry-vulnerability

Soerensen, A. (2019, April 30). *Cyber risk and autonomous ship* . Retrieved from BIMCO : https://www.bimco.org/news/safety/20190430-cyber-risk-and-autonomous-ships

Souli, E. (2020). *Cyber security: A P&I perspective* . Retrieved from The American P&I Club : https://www.american-club.com/files/files/A_Cybersecurity_Perspective_Currents_issue_44.pdf

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

SSM. (2018, February). *Implementation of the EU Genaral Data Protection Regulation 2016/679 - General Guidance*. Retrieved from Steamship Mutual: https://www.steamshipmutual.com/Circulars-London/L.312.pdf

Tam, K., & Jones, K. (2019). Factor affecting cyber risk in maritime. *ResearchGate*.

Walker, J. (2018). *Maritime cybersecurity survey indicates industry is unprepared for risks*. Retrieved from https://www.hellenicshippingnews.com/maritime-cybersecurity-survey-indicates-industry-is-unprepared-for-risks/

World Maritime News. (2018). Retrieved from COSCO shipping lines falls victim to cyber attack: https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/

IV. Insurance Clauses and Rules

American-club. (2020). *Rules 2019/2020*. Retrieved from American Steamship Owners Mutual Protection and Indemnity Association, Inc: https://www.american-club.com/files/files/1920.pdf#page=32

Britannia-P&I. (2020). *Rules-P&I (Class 3)-2020*. Retrieved from The Britannia Steam Ship Insurance Association Limited: https://britanniapandi.com/wp-content/uploads/2020/02/Britannia-Rules-2020-PI.pdf

Gard. (2020). *Rules 2020*. Retrieved from Gard P&I (Bermuda) Ltd: http://www.gard.no/Content/29167884/Rules%202020_web.pdf

IUA. (2003, November 01). *CL601 International Hull Clauses 011103*. Retrieved from International Underwriting Association of London (IUA) : http://iuaclauses.co.uk/site/cms/contentDocumentView.asp?chapter=8&category=57

IUA. (2003, November 10). *CL380 Cyber Attacks Exclusion Clause 101103*. Retrieved from International Underwriting Association of London: http://iuaclauses.co.uk/site/cms/contentDocumentView.asp?chapter=8&category=57

LMA. (2019, November 13). *Lloyd's Market Association Bulletin - Property and Marine Cyber Clauses* . Retrieved from Lloyd's Market Association: https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA19-031-PD.aspx

Japan-P&I-Club. (2020). *Rules 2020*. Retrieved from The Japan Ship Owners' Mutual Protection & Indemnity Association: https://www.piclub.or.jp/attachment/insurance_guidebooks/Rules%202020.pdf

London-P&I-Club. (2020). *Rules 2020/2021 (Class 5)*. Retrieved from The London Steam-Ship Owners' Mutual Insurance Association Limited: https://www.londonpandi.com/documents/the-london-club-pplusi-rules-class-5-2020-2021/

North. (2020). *P&I Rule Book (2020-2021)*. Retrieved from The North of England Protecting & Indemnity Association Limited: https://www.nepia.com/publications/pi-rule-book-2020-2021/

Shipowners. (2020). *The Shipowners' Mutual Protection & Indemnity Association (Luxembourg)*. Retrieved from Club Rule 2020: https://www.shipownersclub.com/publications/club-rules-2020/

Skuld. (2020). *P&I Rules 2020*. Retrieved from Assuranceforeningen Skuld: https://www.skuld.com/contentassets/5cd37a56fa33442baec07c16ee4ac936/2020_skuld_rules.pdf

SSM. (2020). *Rules 2020/2021 Europe*. Retrieved from The Steamship Mutual Underwriting Association (Bermuda) Limited: https://www.steamshipmutual.com/Downloads/Rules-and-Maps-/Current%20Year%20Rules/Steamship%20Europe%20Interactive%20Rules%202020-21.pdf

Standard-club. (2020). *P&I Rules 2020*. Retrieved from The Standard Club Ltd: https://www.standard-club.com/media/3288110/pi-rules-revised.pdf

Swedishclub. (2020). *Rules for P&I insurance 2020/2021*. Retrieved from The Swedish Club: https://www.swedishclub.com/media_upload/files/Publications/TSC_PI-FDD_Rules_2020-2021web.pdf

UKP&I. (2020). *Rules 2020 for UK (Europe), UK P&I N.V*. Retrieved from United Kingdom Mutual Steamship Assurance Association (Bermuda) Ltd: https://www.ukpandi.com/-/media/files/uk-p-and-i-club/products/shipowners/2020-rules.pdf

West. (2020). *Rules of classes 1&2 2020*. Retrieved from The West of England Ship Owners Mutual Insurance Association (Luxembourg): https://www.westpandi.com/resources/?Subject=&Type=Rules