Cyber Risks, Potential Liabilities and Insurance Responses in the Marine Sector

Alicia Aricia Mckenzie

Submitted to Swansea University in fulfilment of the requirements for the Degree of Doctor of Philosophy

Swansea University

2022

THESIS SUMMARY

This summary sheet should be completed after you have read the accompanying notes. The completed sheet should be submitted by you to your Head of Department/School at the time of submission of your work and the supporting documentation.

Candidate's Surname / Family Name : MCKENZIE

Candidate's Forenames : ALICIA ARICIA

Candidate for the Degree of : PhD

Full title of thesis: Cyber Risks, Potential Liabilities and Insurance Responses in the Marine Sector

---

Summary:

The marine sector is vulnerable to cyber-attacks as it becomes more dependent on information and operational technology systems connected to the internet. While this allows for greater efficiency, the interconnected nature of such systems will expose the sector to new and evolving cyber risks.

The research begins by briefly examining the nature of cyber risks, identifying likely threat actors and the motivation behind such attacks. Through the use of hypothetical scenarios, the researcher identified; i) some of the cybersecurity vulnerabilities particular to the marine sector, ii) the potential losses and liabilities from a cyber-attack / incident and iii) analysed how insurance may be used to mitigate the risks focusing specifically on the adequacy of traditional marine policies as well as cyber insurance policies to cover such risks. Traditional marine policies were analysed to identify the gaps in cyber coverage in addition to the recognition that without a clearly written cyber exclusion clause, insurers will be exposed to risks and liabilities they did not intend to cover. As for Assureds, while traditional hull and cargo insurance policies may cover some risk, they will not fully cover losses unique to cyber risks such as network failure, data loss, business interruption, cyber espionage and reputational damage so they too may not have adequate coverage against cyber-attacks.

The main conclusion from the research is that marine and cyber insurance policies currently available do not adequately protect against cyber related losses and liabilities particularly those unique to the marine sector. This is primarily due to the extensive list of exclusions found in cyber insurance policies and commonly used cyber exclusions clauses usually attached to traditional marine policies. The coverage limits are also inadequate to cover the potential losses to marine facilities and assets which are usually connected to a complex supply chain.

DECLARATION

This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed : A. Mckenzie (candidate)

Date: 30 September 2022

STATEMENT 1

This thesis is the result of my own investigations, except where otherwise stated. Where correction services have been used, the extent and nature of the correction is clearly marked in a footnote(s).

Other sources are acknowledged by footnotes giving explicit references. A bibliography is appended.

Signed: A. Mckenzie (candidate)

Date : 30 September 2022

STATEMENT 2

I hereby give consent for my thesis, if accepted, to be available for photocopying and for inter-library loan, and for the title and summary to be made available to outside organisations.

Signed: A. Mckenzie (candidate)

Date: 30 September 2022

Content Page

Acknowledgements

I would like to thank God for keeping me and giving me strength, wisdom and understanding to complete this research.

I also wish to express my sincere gratitude to my supervisors Professor Baris Soyer and Dr George Leloudas for their guidance, useful feedback and encouragement during this research. Many thanks to IISTL members for their support and my PhD colleague, for always believing in me.

To my mother, words cannot express how much I appreciate the sacrifices you have made so that I can achieve my goals. I hope I have made you proud! Thank you.

To my siblings, I hope this will motivate you to be the best version of yourselves.

To the rest my family and all my friends (RP, DT, DW, RC, MW) Thank you.

Table of Cases

Australia Cases

Canada Cases

US Cases

United Kingdom Cases

International Court of Justice Cases

TABLE OF LEGISLATION

United Kingdom Statutes

UK Statutory Instruments

Regulatory Codes of Practice / Guidance

Institute Clauses

Charterparty Clauses

Cyber and other Insurance Clauses

Protection and Indemnity Rules

Table of European and International Legislation

EU Regulation

EU Conventions

International Codes / Resolutions

International Conventions

International General Average Rules

International Organization for Standardization Clauses

Abbreviations

A

ACOW	Additional Cost of Working
AIS	Automatic Identification System
APP	Authorised Push Payment

B

BBR	Beazley Breach Response
BCI	Business Continuity Institute
BI	Business Interruption
BIMCO	Baltic and International Maritime Council

C

CCL	Caribbean Cruise Line
CLI	Cyber Liability Insurance
CRBI	Cyber risk business interruption
CSO	Company Security Officer
CYSO	Cyber Security Officer

D

DPA	Data Protection Act
DOS	Denial of Service
DPD	Data Protection Directive
DPA	Designated Person Ashore

E

ECDIS	Electronic Chart Display and information system

F

FCA	Financial Conduct Authority
FFIEC	Federal Financial Institutions Examination Council

G

GDPR	General Data Protection Regulation
GNNS	Global Navigation Satellite System
GPS	Global Position System

H

H&M	Hull and Machinery Insurance

I

ICC	Institute Cargo Clause
ICO	Information Commissioners Office
ICOW	Increased Cost of Working
IEC	International Electrotechnical Commission
IGP&I	International Group of Protection and Indemnity
IMO	International Maritime Organization
IRS	Internal Revenue Service
ISM	International Safety Management
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISPS	International Ship and Port Facility Security
IT	Information Technology
ITCH	Institute Time Clauses Hulls
ITP	Information Technology Protection

IVCH	Institute Voyage Clause Hulls
IWSCH	Institute War And Strikes Clauses Hulls

K

K&R	Kidnap and Ransom

L

LoH	Loss of Hire

M

MSA	Merchant Shipping Act, 1955
MSC	Maritime Safety Committee
MTSA	US Maritime Transportation Security Act, 2002

N

NCBR	Nuclear Chemical Biological Radiological
NIST	National Institute of Standards and Technology

O

OFAC	Office of Foreign Assets Control
OT	Operational Technology
OTP	Operational Technology Protection

P

P&I	Protection and Indemnity
PCI	Payment Card Industry
PFSO	Port Facility Security Officer
PRA	Prudential Regulation Authority

R

RSCT	Royal Seaforth Container Terminal

S

SCADA	Supervisory Control and Data Acquisition
SDR	Special Drawing Right
SME	Small and Medium Sized Enterprises
SMS	Ship Management System
SOLAS	Safety of Life at Sea
SSO	Ship Security Officer

U

UCC	Uniform Commercial Code
UK	United Kingdom
USA	United States of America
USB	Universal Serial Bus

I. Introduction

A. Cyber Risks and Shipping

1.1. For centuries, shipping has been the most reliable method of transportation and catalyst for trade, connecting commercial markets and industrial hubs across the world. At a domestic level, the UK maritime sector is responsible for '95% of British global trade totalling over £500bn'.[1] The sector's ability to manage such demand is attributable to the technological evolution of the vessels, ports and other marine facilities. Yet, this evolution or increased reliance on technology is equally responsible for the numerous and multiplying occurrences of cyber-attacks /incidents. Cyber risks continue to be listed among the top risks to companies globally, with 44% of the respondents in the Allianz Risk Barometer indicating that cyber incidents are the most important business risks for 2022.[2] It is therefore imperative that the safety of the sector is prioritised as this is critical for economic sustenance and is the main reason stakeholders have found it necessary to develop strategies to manage and mitigate cyber risk. This is succinctly explained in the International Maritime Organization (IMO) Guidelines on Maritime Cyber Risk Management:

> Risk Management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network- based systems has created an increasing need for cyber risk management in the shipping Industry.[3]

[1] Centre for Economics & Business Research (Cebr), 'State of the Maritime Nation 2019' (11 September 2019) 4 < https://www.maritimeuk.org/media-centre/publications/state-maritime-nation-report-2019/> accessed 13 September 2022.

[2] Allianz, 'Allianz Risk Barometer 2022' (Allianz Global Corporate & Specialty) 4 <https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/Allianz_Risk_Barometer_2022_FINAL.pdf> accessed 13 September 2022.

[3] MSC-FAL.1/Circ.3 (5 July 2017). <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf> accessed 13 September 2022.

Against that background, maritime cyber risk refers to the degree to which a threat to technology asset result in a shipping incident or shipping related operational, safety or security failure which is a consequence of the corruption, loss or compromise of information or systems.[4]

1.2. To mitigate the potential liabilities from cyber risks, *BIMCO Guidelines on Cyber Security Onboard Ship*s recommends that along with taking proactive steps 'to identify threats and vulnerabilities, assess risk exposure, developing protection and detection measures, establishing contingency plans and responding to and recovering from cyber security incidents'[5]; companies, ship-owners and charterers must ensure that their liability insurance offers protection against losses arising from a cyber incident.

Vulnerability of the Marine Sector

1.3. The marine sector like all other sectors is not immune to cyber risks, however it is perhaps more vulnerable due to intrinsic weaknesses in the infrastructure and the inadequate training of a high percentage of the human capital employed in the industry. The vulnerabilities include and are based on the extensive use of sensors across the vessel's network[6], high dependence on wifi and satellite based internet systems, over reliance on outdated technology and very low or lack of knowledge of information technology and cyber security among seafarers and other stakeholders.[7] With minimal security protection, communication and entertainment systems onboard vessels are just as vulnerable to cyber risks. Furthermore, the risk of a cyber-attack increases as there is rarely

[4] IMO, 'Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.1)' (14 June 2021) para 1.1 <https://wwwcdn.imo.org/localresources/en/OurWork/Facilit4ation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf> accessed 13 September 2022.

[5] BIMCO and others, 'The Guidelines on Cyber Security Onboard Ships Version 4' (2020). <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships > accessed 13 September 2022. The analysis throughout this research focuses on the insurance aspect of cyber risks and not on the regulatory side of cyber risks. Therefore, the details of these cyber security Regulations, international instruments and Guidelines are beyond the scope of this research.

[6] These include but not limited to vulnerabilities in bridge and engine control systems, internal communication and entertainment systems, anchor and mooring control systems, navigation controls and lights, main and emergency switchboards, power management systems, cargo management systems, access controls and administrative and crew welfare systems.

[7] R. Sen, 'Cyber and Information Threats to Seaports and Ships' in Michael McNicholas (eds), *Maritime Security; An Introduction* (2nd edn, Butterworth- Heinemann 2016) 281-282 <https://doi.org/10.1016/B978-0-12-803672-3.00009-1 > accessed 13 September 2022.

any form of authentication and encryption or even segregation between information technology systems onboard that are connected to facilities ashore[8], an issue made more complex with the network of supply chains that exist in the marine sector. Cybersecurity risks also pose a threat to port and terminal operators as criminals attempt to obtain information on ship schedules, cargo and container details to facilitate cargo and data theft, piracy and or the transport of contrabands and potential attacks from belligerent states. Inadequacies in design, integration and or maintenance of systems on vessels and or at onshore facilities are also vulnerability issues which exposes a marine facility to cybersecurity threats / incidents. Noncompliance or delinquencies in cyber security practices by employees, seafarers and management contributes to the cybersecurity vulnerability of marine facilities.

1.4. The question which may be asked is who would want to attack marine facilities and for what reason? The perpetrators of cyber-attacks on the marine sector will vary depending on the target and the motivation behind each attack. States, members of criminal networks, terrorists, employees, and even private companies determined to achieve or maintain a competitive advantage are all threat actors likely to be responsible for cyber-attacks on marine facilities. The motivation behind these cyber-attacks on the marine sector are mainly for financial (including intellectual property theft) and political gains but more general reasons include dissemination of ideological views, suppress social and political activity or for mere curiosity, accidental errors, or the malicious actions of a disgruntled employee. Politically motivated cyber-attacks on foreign entities and corporations are not novel but the frequency of these types of attacks have magnified since for example, the 2016 attacks on the US Democratic National Committee,[9] the NotPetya

[8] Dennis Bothur, Guanglou Zheng, Craig Valli, 'A Critical Analysis of Security Vulnerabilities & Countermeasures in a Smart Ship System' (Security Research Institute Edith Cowan University 2017) 82 <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1209&context=ism> accessed 13 September 2022.

[9]US Department of Justice, 'Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election' *Justice News* (Washington, 13 July 2018 updated 10 August 2021) <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election> accessed 21 September 2022. Cyber criminals targeted the 2016 U.S presidential elections. Members of GRU, a Russian intelligence agency that is part of the main intelligence directorate of the Russian military were indicted in the District of Columbia for their intended interference with the 2016 U.S. presidential election by targeting the computer networks of the Democratic Congressional Campaign Committee, The Democratic National Committee, the presidential campaign of Hillary Clinton and later releasing related information on the internet.

attacks in 2017[10] and the COVID 19 pandemic.[11] For the first time, the world has experienced a full blown 'hybrid war'[12] where unlike world war I and II, military operations involve both kinetic and cyber-attacks carried out by both state and non-state actors[13] determined to undermine their adversaries and support their allies. Following the invasion of Ukraine by Russia on February 24, 2022, the cybersecurity authorities of US[14], Australia[15], Canada[16], New Zealand[17] and the UK[18] released a joint cybersecurity Advisory, warning organizations both in Europe and abroad that their organizations could be exposed to malicious cyber activity.[19] So far, numerous attacks have been launched against various sectors in Ukraine including distributed denial of service attacks and malware against the government, financial and energy sectors.[20] Russia has not been the lone actor in deploying cyber-attacks against other states. Several cyber-attacks on foreign governments and essential services have been attributed to the Iranian state. Iran was lately chastised for

[10] Andrew Coburn and others, 'Cyber risk outlook' (Centre for Risk Studies, University of Cambridge in collaboration with Risk Management Solutions Inc, 2019) 25 <http://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2019.pdf> accessed 13 September 2022. The impact of the Notpetya attack on container shipping company A.P Moller-Maersk and pharmaceutical company Merck are discussed in scenario 4.

[11] Sam Fenwick, 'Cyber-attacks on Port of Los Angeles have doubled since pandemic' *BBC News* (Los Angeles, 22 July 2022) < https://www.bbc.co.uk/news/business-62260272> accessed 16 September 2022.

[12] Joe Tidy, 'Ukraine says it is fighting first 'hybrid war' *BBC News* (London, 4 March 2022) <https://www.bbc.co.uk/news/technology-60622977> accessed 21 September 2022.

[13] Joe Tidy, 'Anonymous: How hackers are trying to undermine Putin' *BBC News* (London, 20 March 2022) < https://www.bbc.co.uk/news/technology-60784526> accessed 21 September 2022.

[14] Cybersecurity & Infrastructure Security Agency <https://www.cisa.gov/>; The Federal Bureau of Investigation <https://www.fbi.gov/investigate/cyber>; National Security Agency and Central Security Service <https://www.nsa.gov/Cybersecurity/> all accessed 21 September 2022.

[15] Australian Cybersecurity Centre <https://www.cyber.gov.au/> accessed 21 September 2022.

[16] The Canadian Centre for Cybersecurity assessment is 'that Russian cyber operations have tried to degrade, disrupt, destroy or discredit the Ukranian government, military and economic functions as well as take control of critical infrastructure to reduce Ukranians access to information'.
Canadian Centre for Cybersecurity, ' Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine' (22 June 2022) < https://cyber.gc.ca/en> accessed 21 September 2022.

[17] National Cybersecurity Centre <https://www.ncsc.govt.nz/> accessed 21 September 2022.

[18] National Cybersecurity Centre <https://www.ncsc.gov.uk/> and National Crime Agency <https://www.nationalcrimeagency.gov.uk/> both accessed 21 September 2022.

[19] Cybersecurity & Infrastructure Security Agency, ' Alert (AA22-110A) Russian State- Sponsored and Criminal Cyber Threats to Critical Infrastructure' (20 April 2022 revised 09 May 2022) <https://www.cisa.gov/uscert/ncas/alerts/aa22-110a> accessed 21 September 2022.

[20] Microsoft outlines a timeline of cyber operations in Ukraine between December 2021 and April 2022.
Microsoft, ' Special Report: Ukraine An overview of Russia's cyberattack activity in Ukraine' (27 April 2022, Digital Security Unit) < https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd> accessed 21 September 2022.

attacking Albania's government resulting in the destruction of data and disruption of essential services such the booking of medical appointments and enrolment of children in schools.[21] Whereas politically motivated cyber-attacks are on the uptick and quite visible now, corporate espionage appear more dormant, but this does not mean they are not occurring. The reality is companies are always at risks of cybersecurity breaches with some of the perpetrators intending to steal trade secrets and company data. Two Chinese hackers 'were indicted in the United States for conspiracy to commit computer intrusion, wire fraud and aggravated identify theft,' activities which spanned more a decade.[22] They were employed to a science and technology development company in China, were members of a notorious hacking group (Apt 41) and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau. They targeted both government and commercial organisations and stole data, intellectual property and confidential business and technological information from various sectors including aviation, satellite, maritime technology, oil and gas exploration and production inter alia. Another set of hackers from the same group were charged two years later for similar crimes but they also targeted confidential business information including COVID-19 Research.[23] The impact of a cyber-attack is not confined to the targets, there may be spill overs or indirect consequences on the computer system of third-party companies or states who are completely unrelated to the issues.

1.5. These cyber-attacks on businesses appear in various forms and while computer systems are subject to the typical property threats such as fires, floods, and power failures, there are additional threats from hackers, computer viruses, malware, phishing, spoofing, social engineering and threats from cloud computing and the use of smart phones inter alia. Several of these forms of

[21] Foreign, Commonwealth & Development Office and James Cleverly, ' UK condemns Iran for reckless cyber attack against Albania) (7 September 2022, Press release) <https://www.gov.uk/government/news/uk-condemns-iran-for-reckless-cyber-attack-against-albania> accessed 21 September 2022.

[22] US Department of Justice, 'Two Chinese Hackers Associated with Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information' (Office of Public Affairs, 20 December 2018) < https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion> accessed 27 September 2022.

[23] US Department of Justice, 'Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research' (Office of Public Affairs, 21 July 2020) < https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion> accessed 27 September 2022.

attack will be highlighted in the chapters of this research with emphasis on the forms of attack that are the main risks to the marine sector. Along with the threat to vessels and ports, the potential loss from a cyber-attack / incident is magnified when we combine the cyber security vulnerabilities at management offices and those along the supply chain and among customers across the world. Similarly, with each unique type of risks or attack mode, there are potential losses or liabilities to shipowners, charterers, insurers, port authorities and other marine stakeholders. The scenarios and case studies will also highlight many of the liabilities, however the constraints of this research do not allow for the identification of all but only those most likely to be incurred by parties in the maritime sector and where there is uncertainty in terms of insurance of particular types of loss for example regulatory fines. Some of the more common first and third liabilities include breach of privacy events, business interruption loss, cyber extortion loss, cyber fraud, network failure, data and software loss and regulatory fines. Death, bodily injury and physical assets damage though less reported are also potential liabilities from a cyber-attack / incident on a marine facility or vessel.[24] Detailed information on what each liability entails will be discussed in the scenarios.

Current Market Practice

1.6. At the beginning of this research in 2018, cyber insurance was still in its infancy in the UK with many businesses being either oblivious of their risks or vulnerability to cyber-attacks, while others were unaware of the existence of cyber insurance policies. On the other hand, among those who had knowledge of cyber risks, many were of the false impression that their existing commercial policies would respond to the full range of cyber risks to which they were exposed. Gradually, the attitude towards cyber risks has changed which is reflected in more businesses introducing cyber security as part of their safety management systems and recognising the

[24] The scope of this research is limited to nonphysical damage. Therefore, liabilities such as death, bodily injury and physical assets damage will not be discussed at length. This decision was taken after the review of several cyber insurance policies, the majority of which excluded cover for the abovenamed liabilities. This has been one of the most consistent approaches in cyber insurance policy wordings. Therefore, a discussion of these points will be of little value to the research and its intended audience as it is general knowledge among marine stakeholders, with whom the researcher has had interaction throughout the tenure of this research that these risks are usually excluded or offered in limited form in cyber insurance policies. As such, shipowners, charterers and other stakeholders in the marine sector are aware that they must purchase affirmative cyber cover for these losses, usually through a marine cyber hull policy or a cyber write back for these liabilities.

importance of purchasing separate cyber insurance or at minimum an affirmative endorsement clause to their traditional commercial or marine policy. This shift in mindset is the result of a combination of education campaigns, increased cybersecurity training and the publication of major cyber incidents. At the time, the insurance sector had to manage 'silent cyber risk'. This was defined as occurring when insurance policies did not explicitly exclude or cover cyber risks or in more common parlance computer or electronic related risks.[25] Consequently, insurers were exposed to liabilities for cyber incidents they were not prepared or compensated to cover and assureds were inadequately protected because the policies were not designed to cover cyber related risks.[26] The threat of silent cyber exposure was curtailed following the Prudential Regulation Authority (PRA) Supervisory Statement SS4/17[27] and Lloyds Market Bulletin Y5258 (4 July 2019)[28] which mandated that all policies provide clarity regarding cyber coverage by either excluding or providing affirmative cover, with Lloyds directing this be done on or before 1 January 2020.

1.7. Currently cyber insurance cover is provided in three main forms: Standalone Cyber Cover, Affirmative cyber endorsement or a hybrid policy for example a cyber hull marine policy, the latter

[25] Risk Management Solutions, Inc 2016; Managing Cyber Insurance Accumulation Risk; report prepared in collaboration with and based on original research by the Centre for Risk Studies, University of Cambridge <www.jbs.cam.ac.UK/faculty-research/centres/risk/publications/space-and-technology/managing-cyber-insurance-accumulation-risk> accessed 13 September 2022.

[26] An example of silent cyber risks would occur where a hull and machinery (H&M) policy does not include a cyber exclusion or affirmation clause. The shipowner's hull and the cargo onboard the second vessel suffered damage when his vessel collides with an another vessel after his GPS was spoofed. Since there was damage to the hull of the vessel, a claim was made to the H&M insurer. The insurer will initially deny the claim however because there was no exclusion of cyber risks the H&M insurer would be expected to cover the damage to the hull. If there are other losses, for example damage to data or restoration costs, the H&M insurer will not cover these risks so the assured would be inadequately protected. This is prejudicial to the insurers as they did not consider cyber liabilities when the premium was being negotiated. This will be the same outcome for cargo insurers whose policies are silent on cyber risks i.

[27] PRA, 'Supervisory Statement SS4/17: Cyber insurance underwriting risk' (July 2017) 2.1 <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2017/ss417.pdf> accessed 18 September 2022. The Bank of England regulates and supervises financial services firms including insurance companies through the PRA.

[28] Lloyds, 'Providing clarity for Lloyd's customers on coverage for cyber exposures (Market Bulletin Y5258)' (4 July 2019). <https://www.lloyds.com/news-and-insights/market-communications/market-bulletins/?Query=Y5258&Filters=%5B%5D&OrderBy=&Page=1&StartDate=&EndDate=&Type=MarketBulletin&DateChanged=false&HideFields=> accessed 13 September 2022.

being less popular in the market. The assured must choose which is most suitable for the cybersecurity needs of his business based on its risks profile. Affirmative Standalone Cyber policies cover losses, liabilities and other damages arising from information technology breaches whether they be maliciously caused or accidental. Coverage varies, nevertheless they usually cover first and third party risk for 'breach of privacy, data and software loss, network service failure liabilities, forensic investigation of breach, notification cost, reputational damage, business interruption (also without the need for physical damage), regulation and defence coverage, multimedia liabilities, cyber extortion and to a lesser extent physical asset damage (hardware replacement), personal injury and death , intellectual property theft and environmental damage.'[29]

1.8. Another option is Affirmative Cyber Endorsement, these are an extension of a traditional insurance product to include coverage for cyber related losses. The use of cyber endorsement clauses gained momentum in '2017 when around 2-3% of the contracts underwritten at Lloyds included a cyber endorsement clause compared to 2015 when there was no example of affirmative clauses in contracts underwritten at Lloyd's'.[30] An affirmative cyber endorsement clause does not add new risks to the policy, it simply protects and will reimburse the assured for his damage or loss to the original perils for example in their hull policy that is caused directly or indirectly by a cyber-attack /incident. The adequacy of this type of insurance will depend on the scope of endorsement clause, the usual limitation being the distinctive treatment between non malicious and maliciously caused cyber related loss or damage. Endorsement clauses are also criticised for not addressing the bespoke cybersecurity needs of the assured.

1.9. P&I Clubs[31] have agreed to cover liabilities arising from cyber risk to the extent they would have been covered under traditional insurance policies but subject to Club rules where 'there is a common exclusion relating to losses, liabilities, costs and expenses incurred from the use of any

[29] Risk Management Solutions (n 25).

[30] Lloyds, 'Cyber Risks and Exposures: Model clauses- Class of Business Review' (January 2018) <https://www.lmalloyds.com/LMA/publications/modelcyberclausesreviewpdf.aspx> accessed 13 September 2022.

[31] P&I Clubs are independent insurance associations which provide cover for shipowners and charterers against third party liabilities arising from the use and operation of the vessel. The P&I club provides cover for risks and liabilities usually excluded from other marine polices. The liabilities and services covered by P&I clubs include personal injury, loss of life, damage, pollution by oil wreck removal, claims handling and management of maritime casualties. IGP&I, 'About the International Group' (2022) < https://www.igpandi.org/about/> accessed 22 September 2022.

electronic trading system other than those approved in writing by the Club'[32]; 'unlawful, unsafe or unduly hazardous trade or voyage'[33], war risks and terrorism[34]. P&I clubs Biochemical risks inclusion clause 2021 offers a write back of excluded war risk and other liabilities up to a limit of $30 million in aggregate for each ship or any one event directly or indirectly caused or contributed to by or arising from a computer virus or processes as a means for inflicting harm.[35] In the absence of a declaration on the inclusion or exclusion of cyber risks, there was the view that owners and charterers may rely on the omnibus rules in their P&I contracts as the grounds on which they will seek coverage / reimbursement for typical P&I losses / liabilities caused directly or indirectly by computer or electronic risks. The omnibus rule gives the managing committee the discretion to cover 'any liabilities, losses, costs and expenses incidental to the business of owning, operating or managing of a ship provided there shall be no recovery where the loss or damage is caused by a peril that is excluded from the Rules'.[36] It is to be explored later in this research whether insurers will accept claims for cyber-attacks which assureds seek to recover under this clause

Significance and Rationale for Research

1.10. This research is important based on the potential impact of a cyber-attack on the sustenance and economic stability of the maritime sector. Having established the risk and potential liabilities of cyber risks to the marine sector, it is not difficult to envision the benefits of carrying out research on cyber insurance as a mitigating response to cyber threats particularly whether the policies available adequately cover the risk to marine facilities and the industry generally. The research

[32] Example of this Exclusion Clause is Rule 63(j) of Gard Rules 2022 <https://www.gard.no/web/publications/document/chapter?p_subdoc_id=1194646&p_document_id=781871> accessed 13 September 2022.
[33] Rule 74 of Gard Rules 2022 <https://www.gard.no/web/publications/document/chapter?p_subdoc_id=1231457&p_document_id=781871> accessed 13 September 2022.
[34] Britannia P&I, 'Additional Insurances Policy Year 2022 /23: Part IV Clause 4.1 – 4.3' (Version 3.00 (February 2022) < https://britanniapandi.com/wp-content/uploads/2022/02/Additional-Insurances-2022.pdf> accessed 13 September 2022.
[35] Standard Club, 'Bio-chemical risks inclusion clause 2021' (nd) <https://www.standard-club.com/fileadmin/uploads/standardclub/Documents/Import/news/Bio-chemical_risks_inclusion_clause_2021.pdf> accessed 13 September 2022.
[36] The London P & I Club Rules 9.28 < https://www.londonpandi.com/documents/the-london-club-pplusi-rules-class-5-2022-2023-1/ > accessed 13 September 2022.

will look at the traditional marine insurance policies predominantly those that are silent on cyber risks in order to identify the liability exposures to both the insurer and the assured; essentially identifying the gaps in the policies. There will then be an analysis of the current policy wordings and coverage offerings under cyber insurance policies to identify commonly covered risks and those which are most often excluded as well as to identify and discuss the inconsistencies in policy wordings.

1.11. The research will add to academic learning since it includes an in-depth analysis and comprehensive discussions on various aspects of the maritime sector which will be affected by cyber-attacks. Research on this issue is relevant since to my knowledge there is no other study which focuses entirely on the impact of cyber-attack / incident on the marine sector and the adequacy of available insurance policies to protect the assured and mitigate such risks. The research will address cyber risks in relation to the well-established marine insurance concepts such as constructive total loss, safe ports and new issues such as the insurance or noninsurance of regulatory fines that may be imposed after breach of the *UK General Data Protection Regulation / Data Protection Act 2018*. Some sections of the research are written with the objective to increase awareness and encourage open discussion while other areas intended to give a comprehensive view of this evolving risk and its impact on the operation and sustainability of the marine sector.

Methodology

1.12. Throughout this research, hypothetical scenarios and case studies were used to highlight the vulnerabilities, potential liabilities and insurance implications following a cyber-attack or incident on a maritime port facility and or vessels. This method of using scenarios is also useful for testing safety management systems and contingency planning. In each scenario, specific attributes within the marine sector which contributes to its vulnerability to cyber-attacks will be identified. Hypothetical scenarios were chosen as they are best suited to reflect the diverse methods and patterns of attack and are most effective to illustrate the problems or gaps in cyber insurance coverage. Hypothetical scenarios are adaptable which means they can be constantly reviewed and updated to mirror the changes in safety management systems and aid in the identification of

unknown vulnerabilities in these and other systems. The case studies and hypothetical scenarios complement each other, in that they are used to increase awareness among marine sector stakeholders and readers of this research of cybersecurity incidents that have already occurred, how and what caused them and the insurance implications of such incidents. Hypothetical scenarios balances this by introducing to stakeholders 'futuristic' factual patterns what may have not yet occurred, recorded or publicly disclosed. Both methods are used to improve understanding of cybersecurity best management practices, cyber insurance covers and exclusions and gaps in traditional marine insurance in responding to losses or liabilities arising from a cyber incident or attack. The case studies and hypothetical scenarios introduces an element of real life occurrences and are intended to help stakeholders decide how to mitigate their risks and how best to respond if and when a cybersecurity incident occurs.

1.13. The doctrinal legal research method was predominantly used to complete this research. This involved the use and reliance on case law, legislation and legal principles as the foundation of the arguments presented throughout the thesis. Marine insurance principles and that of contract and tort law generally were used to guide the analysis as it relates to cyber risks and insurance in the maritime sector. The reliance on these established legal principles demonstrate that cyber risks and cyber insurance do not alter the principles, even if there are subtle changes or expansion in meaning of key words or phrases. The doctrinal method of research employed by the researcher involved significant periods of library based research relying on secondary sources of law to understand and eventually be able to explain concepts unique to cyber insurance and business interruption. The researcher browsed the websites and knowledge databases of prominent insurance companies, cybersecurity firms, international and government organisation for policy and research on cyber risks which would be useful in the researcher's understanding of the risks and industry and government approach to the management of the cyber risks. Some of the ideas and principles discussed in such research / regulations and best practices guidelines were used to supplement the theories and conclusions made in this research.

1.14. The doctrinal research was complemented by non-doctrinal qualitative approach where the researcher had informal interviews with stakeholders within the marine sector on the issues relating

to cyber risk management and cyber insurance. Multiple meetings were arranged with brokers and insurers to learn about cyber insurance and to understand how the cyber insurance market was developing. The researcher gathered information from stakeholders by requesting copies of cyber and marine insurance policies being offered in the market which were later analysed to identify gaps in insurance for cyber liability. Requests were made by the researcher to brokers and insurers to view and make copies of cyber risks write back options, exclusion clauses and preliminary questionnaires used to assess the risk of prospective assureds and for any other document which would be useful in identifying the inconsistencies and gaps in policies. During these sessions, the researcher had the opportunity to ask questions about terms in the policies that were not very clear and to also understand the intention behind the creation of each clause, how they were to be interpreted and what exactly was expected of the assured. The researcher was also given the opportunity to express her concerns about gaps in coverage and ambiguous language used in some policies and the difficulty this may pose to assureds particularly in the marine sector. These meetings and discussions transitioned to online meetings and continued throughout the tenure of the research so the researcher remain up to date with the trends in the cyber insurance from a practitioner's point of view. Through these meetings and discussions, the researcher was able to gather first-hand knowledge and insight on the current market trends, vulnerability of the marine sector, emerging threats and cyber insurance products. It is this period of collecting and constantly dialoguing with cyber insurance brokers and insurers and other stakeholders in attendance at conferences which cemented the researcher's understanding of the market and confirmed that the case study and hypothetical method of research was the most appropriate method to carry out this research. This data, knowledge and insight was supplemented by library research where journal articles, periodicals, newspaper articles, company and other stakeholder publications on cyber risks, cyber insurance and their impact on the marine sector were read. Most of these documents were retrieved from online searches on company websites and from legal databases such as Lexis Nexis and Westlaw, i-law and Swansea University library database. In addition, there was extensive legal review of current legislation, guidelines and best practices to identify areas that needed modification to address the evolving cyber risk.

Challenges and Delimitation to the Research

1.15. The research is on an area where there is insufficient data to help with the theoretical understanding of the issues, therefore the reasoning applied are taken from general insurance principles and from marine insurance practices. The UK cyber insurance market is relatively young and so there are small numbers of standalone cyber insurance policies and similarly small amount of marine insurance policies with affirmative cyber clauses. Due to a combination of confidentiality and reputation concerns, there was reluctance among insurers and organisations to share insurance policies and data relating to cyber insurance and their cyber risks and safety management profile. To deal with this difficulty, the researcher searched for cyber insurance policies online and downloaded other useful resources from insurance company websites without viewing schedule or policies modified to reflect the needs of specific companies. Furthermore, due to the fact that cyber insurance is relatively new, judgments or arbitrations decisions in this jurisdiction are few, therefore the researcher looked at judgements in more developed markets such as the USA for an understanding of how certain clauses are to be interpreted and applied. While these foreign decisions are not binding on UK firms and courts, they serve a persuasive role since many of the insurance companies here in the UK have subsidiaries or parent companies in the USA which have the same or similar wording as the policies being marketed in the UK. There is further uncertainty about the outcome of cyber insurance cases among businesses in the marine sector since it is expected that many of these cases will be settled out of court in arbitration proceedings or privately paid by insurers to companies that are equally tight-lipped about such proceedings and or payments. These are the very factors which hinder the development of the cyber insurance market and the law surrounding this risk. If all the cases or cyber insurance dispute are decided behind the closed walls of arbitration, courts and judges will never be given the opportunity to question the interpretation, validity and effect of a clause or the adequacy of policy in general. Similarly, the marine sector would not benefit from these decisions since no one will learn except the parties involved in the arbitration, who are under no legal obligation to divulge what was discussed and agreed by the parties. In that sense, development and changes of the policies here in

the UK will linger behind the USA and other markets where the judiciary is involved in development of the product when conflicts emerge between the parties.

Outline and Structure of the Research

1.16. The research is divided in scenarios each named after the most likely forms of cyber-attack on marine facilities and vessels. There are four (4) main chapters: Scenario 1 – Cyber piracy resulting in cyber extortion and ransomware, Scenario 2 – spear phishing and loss of hire and Scenario 3– Onboard Data Breach, Scenario 4- Port Lockdown.

1.17. The first chapter, Scenario 1 highlights new techniques that may be employed by pirates to attack vessels. Modern day pirates have the financial means to collaborate with hackers to simultaneously launch digital and physical attacks on vessels. In scenario 1, the vessel's navigation system was hacked using an inexpensive GPS jammer to reroute the vessel to an area prone to pirate attacks. Pirates entered and captured the vessel while the hackers demanded a ransom. The shipowners agreed to pay the ransom to secure the release of the vessel and protect the crew. The scenario highlights the vulnerability of navigation systems and how easily Global Positioning System (GPS) and Electronic Chart Display Information System (ECDIS)[37] can be hacked and the dilemma of shipowners and charterers when their computer systems are targeted by a ransomware and the safety of the vessel and crew are dependent on the payment of the ransom. The insurance implications of the pirate and ransomware attack is discussed under four (4) subheadings where; i. there is non-exclusion of cyber risks in marine insurance policies, ii. the marine insurance policy includes a cyber exclusion clause and iii. the assured seeks recovery for his losses under his standalone cyber insurance policy or cyber endorsement clause and iv. implications of the cyber piracy under a war insurance policy. A section of this scenario will briefly discuss exclusions and

[37] Global Positioning System 'is a satellite based navigation system comprised of a network or orbiting satellites that provide location and time information, anywhere on or near the Earth.' Electronic Chart Data Information 'provides a continuous, real time plot of the true and relative movements of both the vessel and nearby objects often using images and automatic information system (AIS) transponder signatures superimposed in the electronic chart.' Joseph Direnzo and others (eds), *Issues in Maritime Cyber Security* (Westphalia Press 2017) 398, 5.

possible defences of the insurer where claims are made for the reimbursement of the ransom paid or for the cargo lost or damaged during the cyber piracy attack on the vessel. The very important marine insurance concepts of piracy, constructive total loss, sue and labour expenses and general average contributions will be discussed in relation to repayment of the ransom incurred due to the ransomware attack. P&I and Kidnap and Ransom insurers approach to cyber piracy attack was also discussed in scenario 1.

1.18. The second scenario 2 shifts focus to charterparties issues specifically how a spear phishing attack may lead to loss of hire. Unlike the other scenarios, here the vulnerability or point of entry for the hackers was the parent company onshore. The factual scenario highlights the inability of an employee to recognise a fraudulent email; the opening of which lead to the hackers' malware copying important login details and eventual redirection of hire. It is against this background that the discussion in the scenario concentrates on the fundamentals of a charterparty agreement including the time charterers duty to pay hire. The chapter went on to explore whether the spear phishing attack can be classified as an offhire event? In answering this question, there was a detailed examination of offhire clauses and whether the spear phishing attack prevented the full working of the vessel or whether it can fall under a named offhire event such as deficiency and or default & or strike of officers or crew. Finally, in assessing the insurance implications of the spear phishing attack, the Nordic Plan 2013 version 2016, and the Loss of Charter Hire Insurance Including War (ABS 1/10/83) and Loss of Charter Hire Insurance Excluding War (ABS 1/10/83) clauses were examined to determine their suitability to address cyber risks. A section of the scenario discussed financial institution liability for loss to its customers resulting from a vulnerability in the institutions online services by primarily looking at decisions in the United States of America (US) and forecasting how similar cases may be interpreted in the United Kingdom (UK). Another section of the discussion is in regard to social engineering and computer fraud policies; looking specifically at the courts use of the direct loss test and unauthorised access exclusion to determine whether an insurer should reimburse an assured for losses and liabilities incurred as a result of social engineering or computer fraud.

1.19. Scenario 3 explores the implications of a data breach onboard a vessel. This occurs after an employee inadvertently downloads a malware from the internet which eventually corrupts and destroys all data stored on the ship's system. The main points of the discussion include examining the relationship between a data breach and privacy rights; the nature of a data breach and the obligations thereafter, issues of attribution of liability and whether a data breach can be categorised as a shipping or non-shipping incident in relation to the Convention Relating to the Carriage of Passengers and their Luggage by Sea 1974 (Athens Convention) and 2002 Protocol. Other points in the discussion centres around liability under the regulatory regimes on data breach UK General Data Protection Regulation (UK GDPR) and Data Protection Act (DPA) 2018. The final section of the chapter assessed the insurance implications of the data breach specifically whether traditional marine insurance policies or cyber insurance policies provide adequate protection against losses and liabilities related to the date breach for example notifications costs and potential regulatory fines.

1.20. Scenario 4 Port Lockdown is centred around a hypothetical denial of service attack on the ports of Liverpool. In this scenario, the researcher demonstrated how an outdated unpatched computer operating system is a vulnerability which may result in business interruption at the ports and disruptions along the supply chain. Following prolonged disruptions at the ports, data and cargo loss were reported. The strategic location of the ports, its vital role as a transit hub for cargos and the countless businesses and individuals dependent on its operation increases the risk of aggregation of loss stemming from the main DOS on the port network. Key concepts such as business interruption, cyber business interruption and reputation damage loss were defined. These terms were also analysed in relation to the insurance implication of a cyber-attack on the ports specifically the extent to which the assured is insured against these types of losses either under their standard business interruption policies or their cyber insurance policies.

1.21. At the end of the discussion of the issues in each scenario, the researcher presented bullet summaries of the main points. The overall conclusions and recommendations of the research are presented as main principles with supporting arguments taken from each chapter / scenario. These

are discussed in depth in chapter 5, but the main findings are that 1) traditional marine insurance policies do not adequately protect an assured against cyber risks primarily due to the exclusions added to the policy and or their focus on physical damage and marine perils. 2) Standard marine insurance policies and clauses will not provide adequate cyber protection due to the presence of computer exclusions, the need for loss or damage to be tangible property and cyber risks not generally identified as an offhire event. 3) Cyber liability will not adequately protect an assured against marine loss and damage primarily because of the extensive exclusions and lower limits of liability when compared to traditional marine policies. 4) Standard cyber exclusions clauses relieve insurers of most but not all cyber related risks; therefore, they do not operate as an absolute exclusion. 5) The most adequate cyber protection for an assured in the marine sector will be obtained through a hybrid policy. 6) The lack of standardization in cyber insurance wordings makes it difficult for assureds to understand the extent and scope of their cover and raises doubt about recovery of an indemnity following the loss or damage from a cyber incident / attack.

Scenario 1: Cyber piracy resulting in cyber extortion and ransomware

The ship Orion, while on the high seas was hacked when a malicious program penetrated its navigation system, particularly the Global Positioning System (GPS) and Electronic Chart Display and Information System (ECDIS) and rerouted the ship to a pirate hotspot. The hackers used a very inexpensive GPS jammer to manipulate the ECDIS system by which the hacker intercepted the data between the ship and the satellite system. The pirates attacked and captured the ship and held the crew hostage. A demand was made for £10 million that must be paid in bitcoins to facilitate the release of the ship and crew. To protect the crew members and to secure the vessel, the owners of Orion paid the ransom.

Content **Pages**

I. Cyber Piracy

A. The cyber dimension of piracy

2.1. A cyber pirate, does this even make sense? Few decades ago, the response would have been a resounding no; the combination of words is not logical nor is it a possible occurrence. However, with the advances in technology and the interconnections between vessels at sea and onshore facilities, a cyber pirate attack is no longer just an idea or fantasy but a real possibility and a growing concern among stakeholders within the marine sector. Pirates are taking advantage of this platform and in 2016 exhibited their skills and capabilities when a group of Somali pirates employed hackers to enter a company's IT networks GPS and Global Navigation Satellite Systems (GNSS)[38] to identify ships passing through the Gulf of Aden with valuable cargo and minimal security, thus causing their hijacking to be easier and more profitable. Another incident occurred in 2017, when a master noticed that though his ship was positioned off the port of Novorossiysk in the Russian Black Sea, his GPS was showing his location at Gelendzhik airport which is more than 32 km inland. Several other vessels were similarly affected.[39] The danger is even greater for unmanned vessels which may become easy targets for pirates and cyber criminals, who have the capacity to manipulate the navigational instruments resulting in a collision with another vessel or fixed navigational structure. Though the researcher is unaware of recorded incidents, the hypothetical insurance implications of such an incident will be discussed in parts II - V of this chapter.

2.2. Cyber as a term encompasses 'the interdependent network of information technology (IT) and include the internet, telecommunications systems and embedded processors and controllers in

[38] Global Navigation Satellite Systems is 'the general term that describes any satellite that provides positioning, navigation, and timing services on a global or regional basis'. GPS is owned by the USA and the most prevalent GNSS. GPS.gov, 'Other Global Navigation Satellite System' (last modified 19 October 2021) < https://www.gps.gov/systems/gnss/> accessed 18 September 2022.

[39] Nicholas Newman, 'Cyber pirates terrorising the high seas' (IET, 18 April 2019) <https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/> accessed 18 September 2022.

critical industries.'[40] A cyber-attack 'is any type of offensive manoeuvre that targets IT and Operational Technology (OT) systems, computer networks, and or personal computer devices attempting to compromise, destroy or access company and ship systems and data.'[41] The International Maritime Organisation (IMO) defines maritime cyber risks as 'the measure of the extent to which a technological asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.'[42] The term 'pirate' in marine insurance 'includes passengers who mutiny and rioters who attack the ship from shore.'[43] This description is not very helpful in explaining or identifying the circumstances fit to be categorized as a pirate attack,[44] thus case law will guide us in more accurately deciding whether the facts in this scenario can be described as piracy. While the definition is not comprehensive, it does indicate that unlike theft[45], a person on board the vessel including passengers may be classified as a pirate.[46]

2.3. For an act to qualify as piracy under a marine insurance policy, certain conditions must be met.[47] These include the requirement that the motive behind the attack be for personal gain rather than to promote a political ideology.[48] This distinction was reiterated by Vaughan Williams LJ as he was then, who described a pirate as 'a man who is plundering indiscriminately for his own ends

[40] Hugh Boyes, 'Cybersecurity and Cyber-Resilient Supply Chains' (Technology Innovation Management Review 5(4) 2015) 29 <http://doi.org/10.22215/timreview/888> accessed 18 September 2022.
[41] Bimco and others, 'The Guidelines on Cyber Security Onboard Ships: Version 4' (Annex 4, 2020) <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships> accessed 18 September 2022.
[42] MSC-FAL.1/Circ.3 (5 July 2017) para 1.1. <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf> accessed 13 September 2022.
[43] Marine Insurance Act 1906 (MIA 1906), Schedule 1 rule 8; In Republic of Bolivia v Indemnity Mutual Marine Insurance [1909] 1 KB 785, 789, Pickford J at first instance expressed that 'he is not sure the meaning given for piracy in international law and criminal law are necessarily piracy within the meaning of the term in a policy of insurance.'; Palmer and Another v Naylor and Others (1854) 10 EX 382.
[44] Baris Soyer, *Marine Insurance Fraud* (Informa Law 2014) 201.
[45] Marine Insurance Act 1906; The term 'thieves' does not cover clandestine theft, or a theft committed any one of the ship's company, whether crew or passengers.
[46] *Palmer and Another v Naylor and Others (*1854) 10 EX 382.
[47]These conditions will be briefly explained as there is extensive literature on this topic and is beyond the scope of this paper.
[48] *Republic of Bolivia v Indemnity Mutual Marine Insurance Co Ltd* [1909] 1 KB 785 CA, 796 (Vaughn Williams LJ).

and not a man who is simply operating against the property of a particular state for a public end.'[49] Similarly, the distinction was evident in *Banque Monetaca and Carystuiaki and Another v Motor Union Insurance Co Ltd*[50] where the vessel, Filia was captured by Turkish nationals at knife point. The policy of insurance provided for seizure, but piracy excepted. The point in issue was to determine whether the facts amounted to seizure or piracy? The Court held that the circumstances amounted to seizure and not piracy. Roche J explained that 'Osman Agha was on the side of the Turks and in alliance with the Kemalists in Asia and that he seized and captured the vessel under cover of and largely upon motives of a political character.'[51] This should not be interpreted as there being zero motive for personal gain, instead what was underscored in the judgment of Roche J was that 'the action that led to the capture and seizure of the vessel was predominantly political and military.'[52] This according to Roche J changed it from the position of piracy within the meaning of the clause.

2.4. Furthermore, there must be some degree of force if piracy is to be established. The act or threat of force must be exercised before the appropriation is completed.[53] In *The "Andreas Lemos"*[54] a gang of men armed with knives went onboard the vessel while it was at anchor. The criminals stole equipment including mooring ropes and when confronted by crew members who were themselves armed, the criminals brandished their knives in defence and to facilitate their escape. The court held this was not piracy as force or threat of force was used only after the criminals stole equipment from the vessel. Staughton J explained that insurance coverage for piracy is provided on the basis that 'loss has been caused to the ship owners because their employees are overpowered by force or terrified into submission.'[55] He emphasized that 'the notion of piracy is inconsistent with clandestine theft.'[56] In the absence of force the ship owners could not recover from their insurers for loss due to piracy. Additionally, it will not suffice if the

[49] ibid 796.

[50] Banque Monetaca and Carystuiaki and Another v Motor Union Insurance Co Ltd (1923) 14 LIL Rep 48.

[51] Ibid 50.

[52] ibid 51.

[53] *Athens Maritime Enterprise Corporation v Hellenic Mutual War Risks Association (Bermuda) Ltd (The "Andreas Lemos*" [1982] 2 Lloyds's Rep 483, 491.

[54] Ibid.

[55] Ibid.

[56] *The "Andreas Lemos"* (n 53) 491.

violence used by the attackers was only directed against property, for unlike theft there must be use of force against the crew or master.[57] A definition of piracy which incorporates all the elements is "forcible robbery at sea, whether committed by marauders from outside the ship, or mariners, or passengers within it. The essential element, however, is the voluntary dispossessing of the master and afterwards carrying away the ship itself, or the whole or part of the cargo, with felonious intent."[58] The law on what constitutes piracy in the traditional sense is settled, however the dynamics of modern day piracy, particularly those with a cyber element may put the established rules to test. Force is a prerequisite of the act of 'piracy' but there is doubt as to the extent to which a cyber-attack will satisfy this requirement so that the existence or non-existence of a cyber element will decide or change the classification of the act.

2.5. For the purposes of this thesis, a cyber pirate attack consists of hackers and pirates working together to manipulate the information and operational technology including the navigation systems onboard a vessel to steer it to a location that makes it easier for the pirates to attack and rob the vessel. Against this background, the questions worthy of examination are whether such an attack will be considered piracy in accordance with the principles of marine insurance and whether insurers are willing to cover the liabilities resulting there from? The insurance implications of this scenario will be analysed from three perspectives; firstly, where there is non-exclusion of cyber risks more commonly referred to as silent cyber risks; secondly where cyber risks have been explicitly excluded in the traditional marine insurance policies held by the assured and thirdly where the assured has a standalone cyber insurance policy.

B. Identification and classification of the peril - Piracy?

2.6. The vessel Orion was hacked by cyber criminals and captured by pirates while it was located on the high seas. There are two dimensions to this incident, there is the cyber-attack by the hackers

[57] Baris Soyer, *Marine Insurance Fraud* (Informa Law 2014) 205; *Suez Fortune Investments Ltd v Talbot Underwriting Ltd (The Brilliante Virtuoso)* [2019] EWHC 2599 (Comm) "I have been referred to no authority to suggest that theft from an unattended vessel on the high seas amounts to an act of piracy. On the contrary, the above cases and those referred to in them all concerned acts perpetrated against manned vessels. The strong implication from the decisions is that piracy requires the threat or use of force against persons not simply against property…" [para 77] (Ms Julia Dias QC sitting as a Deputy High Court Judge).

[58] *Republic of Bolivia v Indemnity Mutual Marine Insurance Co Ltd* [1908-10] All ER Rep 260, 268.

whose motive and location are unknown and there is the abduction of the vessel and crew by the pirates. With that said, can the facts herein satisfy the requirement of a 'peril of the sea' even if the GPS and ECDIS of the Orion were penetrated by hackers who were miles away on land? 'Perils of the sea' is defined in Schedule *7* of the *Marine Insurance Act 1906 (MIA 1906)* and 'refers only to the fortuitous accidents or casualties of the seas but does not include the ordinary action of the winds and waves'. Perils of the sea include damage to goods caused by the accidental incursion of sea-water, storms, stranding, collisions and other perils peculiar to the sea or to ship at sea which could not be foreseen and prevented by the shipowner with reasonable care.[59] The cases establish that not all accidents or casualty which occur on the sea will be perils of the sea, creating a distinction between what occurs 'on the sea' and what is 'of the sea'.[60] In *P. Samuel and Company Ltd v Dumas*, the point was made that the scuttling of the vessel occurred on the seas but was not a peril of the seas and it was due to the fraudulent and deliberate act of the owner, which is not an accident or fortuitous.[61] The same point was made in *Canada Rice Mills, Limited Appellants v Union Marine and General Insurance Company, Limited Respondents* when the ventilators in the ship's hold had to be closed for brief intervals so the rice could be protected from the rain. The comment was made that the rain was not a peril of the sea but was a peril on the sea even though it was eventually decided that the rain was not the cause of the damage to the rice.[62] The proximate cause of the damage to the rice was found to be the deliberate and reasonably necessary closing of the valves to protect the rice from being affected by the peril of the sea. The court held that even though it was not the incursion of the water that caused the damage, the act taken to prevent the incursion is a peril of the sea thus the loss was due to a peril of the sea.[63] The cyber-attack on its own would not fit into the definition of perils of the sea, however if the cyber-attack has caused a peril such as the incursion of water that leads to damage or piracy as the proximate cause of the loss, the cyber-attack would qualify as a peril of the sea. Nonetheless, peril of the sea is not limited to incidents involving harsh or unforeseen weather conditions or loss

[59] Scrutton on Charterparties and Bills of Lading (24th edn, Sweet & Maxwell 2019) 11-058.
[60] *Thomas Wilson, Sons and Co v The Owners of the Cargo per the "Xantho"* (1887) 12 App. Cas. 503, 509.
[61] [1924] A.C. 431, 454, 458 and 465.
[62] [1941] A.C. 55, 64.
[63] [1941] A.C. 55, 70 -71; *Stanley v Western Insurance Co. (1868) L. R. 3 Ex. 71* , 74; *P. Samuel & Co. v Dumas* [1924] A. C. 431

because of an unseaworthy vessel, what is necessary is 'anything that will count as a fortuitous external accident or casualty'.[64] Some writers disagree that a cyber-attack could be characterised as a peril of the sea. Professor Bulent Sozer expressed the view that to qualify as a peril of the sea, the event must be peculiar to the sea or ship at sea. He reasoned that since cyber-attacks are not peculiar to the sea nor do they originate in the sea, they cannot be properly characterised as perils of the sea acknowledging instead that they are perils on the sea.[65]

2.7. By applying sections 2 and 3 of the *MIA 1906* and related cases to answer the question, it would mean that even if the hackers location was on land, because their act was directed at the Orion while it was at sea, the incident directly affected a marine adventure which led to the piracy, one of the enumerated maritime perils mentioned in section 3 of the *MIA 1906*[66] and that which is consequent on or incidental to the navigation of the seas. It was decided in the *Captain Panagos* that in determining whether the *MIA 1906* applied to a peril which caused a loss to the assured the real question is not whether the peril (in this scenario the cyber-attack) resembled the perils listed in section 3 but rather, whether the peril is consequent on or incidental to the perils of the sea.[67] The phrase 'consequent on or incidental to the navigation of the seas' is mentioned in the section 3 of the *MIA 1906* where it was used to define maritime peril while the scope of the Act was explained in the subsequent sections. In a contract of marine insurance 'the insurer undertakes to indemnify the assured …. against marine losses which is defined as losses incident to a marine adventure'.[68] A marine adventure occurs 'when ship goods …...are exposed to maritime perils… perils consequent on or incidental to the navigation of the seas, … and any other perils…. which may be designated by the policy'.[69]

---

[64] *Global Process Systems Inc and Another v Syarikat Takaful Malaysia Berhad (The "Cendor Mopu")* [2011] UKSC 5; [2011] 1 Lloyd's Rep. 560, 580.

[65] Bulent Sozer, 'Seaworthiness: In the Context of Cyber-risks or "Cyberworthiness" in Baris Soyer and Andrew Tettenborn (editors), *Ship Operations: New Risks, Liabilities and Technologies in the Maritime Sector* (2021, Routledge), para. 4.1.2.

[66] "Maritime perils" means the perils consequent on, or incidental to, the navigation of the sea, that is to say, perils of the seas, fire, war perils, pirates, rovers, thieves, captures, seizures, restraints, and detainments of princes and peoples, jettisons, barratry, and any other perils, either of the like kind or which may be designated by the policy.

[67] '*The Captain Panagos D.P' [1985*] Vol. 1 Lloyds Rep. 631, 632 (Mustill J).

[68] MIA 1906, s 1 (my emphasis added).

[69] MIA 1906, s 3 (2).

2.8. Mustill J in *The Captain Panagos DP* stated '... The closing words 'and any other perils…which may be designated by the policy' does not mean that the inclusion of 'any peril' would qualify the contract as a marine insurance policy to which the *MIA 1906* would apply.'[70] *Rule 12 of Schedule 1* of the *MIA 1906* states that 'the term "all other perils" includes only perils similar in kind to the perils specifically mentioned in the policy'. A simple explanation for this reasoning can be found in one of the well-established rules of interpretation, 'noscitur a sociis' which states that use of general words may be limited by the subject matter to which it is related. Another rule 'ejusdem generis', provides that where there is a general term which is preceded by a list of specific words, that general word must take a similar meaning or fall within the same genus as the specific words, so any peril that will be covered under the *MIA 1906* and *IA 2015* must be limited by the words such as 'incidental to the navigation of the seas' and of similar type as the maritime perils listed in section 3 of the Act.[71] It was further decided by Mustill J that; 'The form of the policy or the fact that all the perils listed in *MIA 1906* are covered is not sufficient, but as aforementioned is a marine policy if the perils insured are consequent on or incidental to the navigation of the sea'.[72] There is no clear explanation of the meaning of the phrase 'consequent on or incidental to the navigation of the seas.' However, based on the foregoing a cyber incident will not be covered under a marine insurance policy if there was no marine adventure which suffered loss due to a maritime peril. A cyber-attack on its own is not peculiar to the sea. This conclusion is subject to the intention of the parties and the express words of the contract. Similarly, the meaning given to the words used will be subject to trade customs within the maritime industry. Accordingly, these rules of interpretation will function as a barrier, to prevent very general words and every type of incident at or on the sea from being referred to as a peril of the sea or that which is consequent on or incidental to the navigation of the sea. Consequent on and incidental to the navigation of the seas does not mean that the peril in this case, the malicious penetration of the

[70] [1985] 1 Lloyd's Rep.625 (emphasis added).

[71] *Thames and Mersey Marine Insurance Co. v Hamilton, Fraser & Co* (1887) 12 A.C. 484. 501; *Hamilton, Fraser & Co v Pandorf & Co.* (1887) 12 App. Cas. 518, 523 (Lord Halsbury) '… it must be admitted that words may receive a limited meaning by reason of the other words with which they are associated, or by reason of the subject-matter with which they deal, or by reason of the mode in which they are commonly used.'

[72] '*The Captain Panagos D.*P' [1985] 1 Lloyd's Rep.625, 631,632 (emphasis added).

ECDIS and GPS of the Orion can only occur on the seas. All that is required by these words is that a substantial part of the marine adventure / voyage takes place upon the seas.

2.9. *MIA 1906, section 2(1)* provides that '…. marine insurance contract may by express terms or usage of trade be extended to……. losses on inland waters or any land risks …. incidental to any sea voyage.' 'Incidental to any sea voyage' means a greater percentage of the voyage has taken place at sea as compared to the other mode of transportation utilized during the voyage. There is no mention made of any land journey in the scenario, yet it will be assumed that even if there had been a land journey covered by the insurance policy, it was miniscule in comparison to the extent of the sea leg of the voyage. In any event, our concern here is about the cyber risks and whether the location of the hackers would prevent their act from being recognized as an incident at sea. The response to this concern is impacted by the nature of cyber risks. Cyber risks are not limited to a geographical space therefore an attack perpetrated by hackers who are located on land can affect businesses, vessels, and operations in different spheres. This means that the cyber-attack may affect land, air and sea operations, therefore it is difficult to isolate or categorise a cyber - attack as merely a land risk or alternatively a peril consequent on or incidental to the navigation of the sea. Yet, this unique feature does not prevent cyber risks from being recognized as a peril which is consequent on or incidental to the navigation of the seas. The point is more apparent with the high dependence of vessels and marine onshore facilities on technology which increases the vulnerability of these and other marine systems to cyber-attacks. Furthermore, if the authorities intended for the phrase 'consequent on or incidental to the navigation of the seas' to mean perils which could only occur at sea, the non-exhaustive list of perils named in section 3 of the *MIA 1906* would be contrary to that intention. In other words, the fact that the policy covers risk which may only occur on land does not mean it is uninsurable under a marine policy[73], however this is not an issue with cyber risk as the peril can occur in any environment provided there is some interface between the operation of the business and networks connected to the internet. Acknowledging that the hackers may be located on land while the ship is being attacked at sea distinguishes it from the peril of theft in the sense that unlike theft, a cyber-attack will still be recognized as such even if

[73] Robert Merkin, 'Marine Insurance Legislation' (Johanna Hjalmarsson, Aysegul Bugra and Jennifer Lavelle (eds), (5th edn, 2013).

the perpetrators came from outside the ship or the act was committed by someone who was already on the ship such as crew or passengers.[74]

2.10. Another issue which is impacted by the nature of cyber risks is the difficulty in locating the origin of the attack. It is easy for us to imagine the hackers of the Orion sitting in a land-based room around a computer, however would the attack become a risk 'incident to the sea' if the hackers were actually onboard the vessel of the pirates? The hackers location is immaterial but hypothetical scenarios must not be limited to hackers or cyber criminals being completely detached or in a different location from the marine assets. The more important point is that the hackers were hired to target the Orion, an attack executed while the Orion was at sea to facilitate the activities of the pirates. Even if the attack was carried out within the territorial waters of a state, the act would still amount to piracy, provided there was use of force and in pursuit of personal gain. Since the operation of vessels like the Orion depend extensively on many networks which are continuously connected to the internet, the risks of a malicious invasion of cyber- attack increases.

2.11. Whether the requirement that force be used for an act to amount to piracy is fulfilled is debatable in this scenario. The form of action which will qualify as force has not been determined in cases, however clandestine theft or stealth[75] will not be categorised as piracy. There needs to be an element of physical force. A cyber-attack of this kind cannot be described as clandestine theft. While it is accepted that the hackers did penetrate the computer and navigations systems onboard the Orion in an unnoticeable manner, this should not be enough to discard the act in its entirety from being categorised as piracy. The pirates used the technological flaws on the Orion to their advantage to increase their chances of success. Whether a cyber-attack can be classified as 'force' in the physical sense of the word will depend on the effect it has on property or person to which it is directed. If the cyber-attack causes physical damage of the magnitude equivalent to what would have been caused by a physical, kinetic, biological or chemical attack, it is possible that the cyber-attack will be deemed as the use of force. On the other hand, if there is no physical damage, an

[74] This contrasts with how theft is interpreted in marine insurance. According to rule 9 of schedule 1 of the MIA 1906, "The term "thieves" does not cover clandestine theft or a theft committed by any one of the ship's company, whether crew or passengers."

[75] *The "Andreas Lemos"* [1982] 2 Lloyds's Rep 483.

element of force may be ascertained based on major disruptions with IT and OT systems and the eventual interference with business operations or the functionality of critical infrastructure.[76] A discussion of the effect of Stuxnet worm which affected several industrial control systems in Iran, but no evidence of physical damage examined whether use of force exists in that context. It was decided that Stuxnet's impact on the economic value the uranium products and Iran's nuclear programme would not be considered 'use of force' with regard to Art 2 (4) of the Charter of the United Nations.[77] Another important point was that though Stuxnet was designed to amend, suppress, delete or send data and not cause kinetic effects equivalent to that of traditional weapons, its effect may still be classified as 'armed force' 'if it is comparable to the effect of kinetic, biological or chemical weapons' with keen emphasis on the severity of these effects.[78] The consensus was that the effect of Stuxnet, that is the non-trivial destruction of property would determine whether the Stuxnet worm constituted 'armed force'. Even if the main effect was on the supervisory control and data acquisition (SCADA) systems and there is no evidence of 'physical' destruction, the effects of Stuxnet should still be deemed 'use of armed force' if critical infrastructure in Iran was substantially disrupted.[79] Some have even expressed the view that the 'destruction of data that is of substantial importance and economic value' could also be classified as 'armed force'.[80] Customarily, economic or political coercion has not been accepted as use of force, and this is demonstrated in the decision of *the International Court of Justice* in the

[76] For a detailed discussion of cyber-risks and the use of force based on principles of International law, see chapter 2: 'Cyber Operations and the jus ad bellum' in Marco Roscini , *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014) and Michael N Schmitt, 'The Use of Force: Rule 69' in Tallin *Manual 2.0 on the International Law Applicable to Cyber* Operations (2nd edn, Cambridge University Press 2017) A non-exhaustive list of factors to consider when assessing whether a cyber operation amounts to use of force include: its severity, immediacy, directness, invasive, measurability of effects, military character, state involvement and presumptive legality, identity of the attacker and the nature of attacker inter alia. The Tallin Manual is a good but nonbinding legal source which explains how international law applies to cyber operations. It is in the process of a five (5) year review for the launch of Tallinn Manual 3.0

[77] Katharina Ziolkowski, 'Stuxnet – Legal Considerations' (CCDCOE 2012) 9.
< https://ccdcoe.org/uploads/2018/10/Ziolkowski_Stuxnet2012-LegalConsiderations.pdf> accessed 18 September 2022.

[78] Katharina Ziolkowski, 'Stuxnet – Legal Considerations' (CCDCOE 2012) 9 – 10.
< https://ccdcoe.org/uploads/2018/10/Ziolkowski_Stuxnet2012-LegalConsiderations.pdf> accessed 18 September 2022.

[79] Ibid 10-11.

[80] Ziolkowski (n 78)10 citing J. Barkham, Information Warfare and International Law on the Use of Force, in: Vol. 34 New York University Journal of International Law & Politics 2001, 72.

Nicaragua Case of 1986.[81] Therefore from an international law perspective, a ransom will possibly be classified as an economic coercion rather than use or threat of the use of force, however this may change considering the potential destabilising effect or economic damage that may arise from a cyber-attack.

2.12. Since there was both a digital and physical attack on the vessel, it is the events that occurred after the vessel arrived in the pirate hotspot which should be the focus of whether a pirate attack has occurred. As distinct from the position in *The* '*Andreas Lemos'*, the facts here suggest that the pirates attacked and captured the vessel and crew then made a demand for ransom. Whereas the exact form of physical action was not depicted in the facts, by the use of the word 'attack' to describe what occurred, the inference can be made that some amount of force was exerted by the pirates and directed at the crew to capture and seize the vessel by the pirates due to the use of the word 'attack' to describe what occurred. The natural and ordinary meaning of the word 'attack' is 'coercion or compulsion, especially with the use or threat of violence'[82] so this implies that there was use of force and the instilment of fear among the crew especially when they were being held for ransom.

2.13. An alternative argument is that since information and operation systems are becoming increasingly interconnected and as cyber criminals commit to breach these systems, it is perhaps time for the courts/ marine sector to revise and broaden the meaning given to 'force or threat of force'. This is on the premise that soon, there will be very few immediate or direct contact between criminals and crew or even the vessel. If the requirement of force or violence retain its narrow meaning, it will become impossible for an event to be labelled theft or piracy and accordingly would deny assureds of any claim for their loss against insurers in such circumstances. It is suggested therefore that as it relates to cyber-attacks in furtherance of piracy or seizure, to decide if there was the use of force the parties may consider; the effect of the cyber- attack, the criminals' intent to control the computer systems and the capture of Orion and its cargo against the will of

[81] ICJ, *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America),* Merits, ICJ Reports 1986, para 245.

[82]*Oxford English Dictionary* (OUP 2019) < https://www.lexico.com/en/definition/force> accessed 18 September 2022.

the crew. Moreover, cyber criminals gain unauthorised access to the vessel's computer systems and developed malicious codes to unlock passwords and other security IDs implemented to protect physical and digital networks. Therefore, it is beneficial to examine the effect of the cyber-attack and the intent of the hackers, a difficult task considering the challenges of identifying the perpetrators of cyberattacks. Such analysis introduces a criminal standard into cyber insurance procedures however the reality is that the hackers are committing a criminal offence which may be better understood by transfer of skills and knowledge from criminal law. This cannot be a blanket approach as introducing the criminal standard of 'beyond a reasonable doubt' into an insurance clause will further complicate the claims process but such method is not foreign to the insurance sector as this has already been the required standard for specific clauses in some cyber insurance policies (though not a marine cyber insurance policy).[83] In those instances, it would not be unusual for the assured to be required to provide forensic evidence of their computer system which has been hacked along with searches of social media websites and financial records including any cryptocurrency accounts which may have been used to facilitate money transfer or purchases of hacking tools sold on the black market. These are additional evidence which the insured may be required to establish before an insurer will pay for any claim that must be proved beyond a reasonable doubt.

2.14. Even with the introduction of the criminal standard in marine cyber insurance clauses, there is still uncertainty as to whether this will deter pirates from partnering with cyber criminals to attack and detain vessels. It is already a challenge for governments to control piracy. The task will be made more difficult as the higher the success rate of the pirates working with cyber criminals, the greater the likelihood that incidents of this nature will continue to rise. A real concern is to determine the most effective means of intercepting these cyber-attacks since besides maintaining a good cyber hygiene, there is no real defence or prohibitive measures in place to prevent hackers

[83] For example Tokio Marine HCC Cyber Security Insurance Policy 0417 Clause 2 Notification Costs; 'The Insurer agrees that, if during the Period of insurance the Insured suffers a Claim, Loss or notifies of a Circumstance under Insuring Section 1.1 or becomes legally obliged to notify in order to comply with Data breach law, that the Insurer will pay the reasonable and necessary costs incurred by the Insured to draft, send and administer notification communications to those whose data, following forensic investigation has, or beyond reasonable doubt has been stolen, misplaced or compromised.'

and pirates from working together to successfully take control of vessels. It is expected that piracy will no longer be concentrated along notorious coastlines or attack zones such as the Gulf of Aden and Guinea but quite likely will develop in territories once considered safe havens against the threats of piracy. This may develop quickly within territories of countries whose nationals and governments have invested heavily in cyber security and technology such as Iran, China and Russia all of which are located within sea zones not particularly linked to many pirate attacks. The same cannot be said about the government relaxed attitude to the many cyber-attacks which have been attributed to persons living and operating within their domain. Under these conditions, businesses will operate in constant fear of being victims of cyber-attacks either because of the immediate financial loss or the reputational damage to the company. Accordingly, the requirement of force must be construed to reflect the commercial realities that cyber risks will often not fit into the classical definition of 'force' which requires use of threat or physical violence thus should not be applied to disqualify malicious electronic and computer hacks from meeting those requirements. A similar point was considered by Prof Bulent Sozer when he responded to the question of whether a cyber-attack can qualify as 'piracy'. He concluded that this was unlikely since an essential element of piracy is the use of physical force at sea whereas cyber- attacks operate in virtual realm thus does not satisfy this main element.[84] While the researcher agrees with Prof Bulent Sozer's analysis, the researcher is respectfully of the view that his conclusion is limited to those scenarios where a cyber-attack is carried out on its own without the involvement of pirates at sea. In the latter case, as mentioned above the cyber-attack which leads to a pirate attack, collision or any other peril and is an efficient cause of the loss may in some instances be categorised as a peril of the seas.

2.15. Another important point is the issue of the legality of paying the ransom. Ransom payments are not illegal in England and Wales provided they are not paid to or have any association with terrorist groups[85], persons subject to economic sanctions or used to finance a criminal act and there

[84] Bulent Sozer, 'Seaworthiness: In the Context of Cyber-risks or "Cyberworthiness" in Baris Soyer and Andrew Tettenborn (editors), *Ship Operations: New Risks, Liabilities and Technologies in the Maritime Sector* (2021, Routledge), para. 4.1.2.

[85] Terrorism Act 2000, s. 15(3); Serious Crime Act 2007, ss 45- 46.

is nothing illegal about the contracts between the parties.[86] The National Cyber Security Centre (NCSC) in their guidance on mitigating malware and ransomware attacks emphasised that law enforcement does not encourage, endorse or condone the payment of ransom demands.[87] Notwithstanding, insurers continue to provide ransom to protect assureds against the constant threats to vessels and crews from pirates and now cyber criminals. However, insurers are prohibited from paying a claim if they know or have reasonable cause to believe that the ransom will be paid to terrorists or for the purposes of terrorism.[88] In such circumstances, the insurer must notify the National Crime Agency of its suspicion. Prudential Regulation Authority (PRA)[89] Fundamental Rule 7 obliges a firm / insurer to disclose to the PRA anything relating to the firm which the PRA would reasonably expect notice, a ransom demand would certainly be fall into this category.

2.16. The legality of the payment of ransoms will determine the product options offered by insurers. There is a reluctance to ban ransom payments because of the need to protect the rights of private citizens and businesses who may be held at ransom. The refusal to pay could result in a choice between life and death and the solvency or insolvency of a business.[90] As such, governments have instead imposed restrictions on the circumstances under which a ransom payment will be allowed while insurers have demanded that their customers maintain an up to date cyber management system and abide by the recommended best management practices for piracy. The U.S Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory on the risks of sanctions for facilitating ransomware payments, but the US has not

[86] Serious Crime Act 2007, ss 45- 46.
[87] NCSC, 'Guidance: Mitigating malware and ransomware attacks' (Version 3.0, 09 September 2021) < https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks> accessed 18 September 2022.
[88] Terrorism Act 2000, s. 17A (1); Counter-Terrorism and Security Act 2015, s. 42(1).
[89] The Bank of England regulates and supervises financial services firms including insurance companies through the PRA.
[90] Colonial Pipeline Company, US largest refined products pipeline was the victim of a ransomware attack in May 2021 which caused the company to shut down its system for more than 30 hours. Colonial paid the cyber criminals (Darkside) approximately 75 bitcoins valued at $4.4 million to release the system which they made a claim to recover from their cyber insurers. The U.S authorities were able to trace and recover 63.7 bitcoins valued at $2.3 million of the ransom that was paid to Darkside.
ICC Commercial Crime Services, 'Clampdown against cyber criminality' (n.d) <https://www.icc-ccs.org/index.php/1307-clampdown-against-cyber-criminality> accessed 18 September 2022.

outlawed the payment of ransoms.[91] The advisory warned that companies including insurance firms, financial institutions and those specialising in digital forensics and incident response that facilitates the payment of ransom may risk breaching OFAC Regulations. These companies are encouraged to contact the relevant government agencies if they reasonably believe that the person making the ransom demand may be sanctioned or is in connection with sanctioned individual or entity.[92]

2.17. The main loss to the assured shipowner's is the ransom paid to the pirates to secure the release of the vessel, crew and the cargo onboard. The usual procedure is for the assured to have the money released from their insurers and the assured shipowner of the Orion would arrange for the delivery of ransom monies to the pirates, however in this scenario, the request is for bitcoin transfer which means it is expected that the assured has access to bitcoin reserves, otherwise this would further delay the release of the vessel and crew. The requirement for the ransom to be paid in bitcoins was an attempt by the hackers to conceal the parties involved in the transaction. Yet, bitcoin transactions are highly transparent and except where added steps are taken to anonymize the transactions, they are traceable and are saved on public ledgers called blockchains. The identity of the user behind an address is kept private but revealed during a transaction hence the reason it is recommended not to reuse a bitcoin address and to use multiple wallets for each transaction.[93] Unlike Bitcoin, Monero which is another type of cryptocurrency would pose more problems as these are untraceable. Each Monero transaction is private, and each user is anonymous by default. Monero uses three technologies to achieve such levels of anonymity: stealth address which hides

[91] The U.S. Department of the Treasury's Office, 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments' (OFAC, 01 October 2020)
< https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf> accessed 18 September 2022.

[92] *Mamancochet Mining Limited v Aegis Managing Agency Limited and Others* [2018] EWHC 2643(Comm); [2019] 1 All ER (Comm) 335, paras 49-50.
In interpreting the meaning of a sanction clause in a marine cargo policy with the phrase 'to the extent that '…payment of such claim …would expose that insurer to any sanction, prohibition or restriction under …the trade or economic sanctions, laws, or regulations', the court held that in order for an insurer to refuse to pay a claim, they must show that doing so would expose the company to sanctions law and not merely expose the company to the risk of being sanctioned…'

[93] Bitcoin, 'Protect your privacy' (2022) < https://bitcoin.org/en/protect-your-privacy> accessed 18 September 2022.

the sender[94], ring signatures obscures the receiver[95] and RingCT hides the amount of the transaction.[96] Notwithstanding the traceability of Bitcoins, cyber criminals continue to request ransoms or ransomware payments to be made in bitcoins. *AA v Unknown and others*[97] is a UK case which illustrate the upward trend of ransoms being requested in cryptocurrencies. The claimants were UK insurers whose customer, a Canadian insurance company, computer system was hacked and encrypted. Ransom demands of US$950,000 in bitcoins to a specific address was made by the hackers before the system would be decrypted. The Claimants agreed to pay the ransom. Some of the money was transferred into fiat currency while 96 bitcoin was sent to an address linked to an exchange operated by the 3rd and 4th defendants. The first Defendant was the persons unknown who made the demand. The second Defendant was the owner / controller of the 96 Bitcoins. The insurers contracted the services of an incident response company that specialises in the negotiation of crypto currency ransom payments to negotiate with the hackers to regain access to its data and systems. Based on the importance to the customer of regaining access to its system, the assured decided to pay the ransom so they could obtain the decryption tool.[98] Parts of the negotiation are reproduced below to highlight that there have been instances where UK insurers have agreed to pay ransom demands in cryptocurrencies.

The initial text from the hackers on the customer's computer is reproduced below:

---

[94]Stealth addresses allow the sender to create one-time addresses on behalf of the receiver for each transaction. The recipient will publish one address while each payment is sent to a unique address on the blockchain which cannot be linked to any other transaction. With stealth addresses, only the sender and receiver can figure out where the payment was sent.
Monero, 'Stealth Address' (Moneropedia, 2022)
< https://www.getmonero.org/resources/moneropedia/stealthaddress.html > accessed 22 September 2022.

[95] This is a type of digital signature that can be performed by any member of a group of users that each have keys so that the signature could be from anyone in the group and it is impossible to identify who produced the signature. This features ensures that transactions are untraceable.
Monero, 'Ring signature' (Moneropedia, 2022)
< https://www.getmonero.org/resources/moneropedia/ringsignatures.html>accessed 18 September 2022.

[96] RingCT is abbreviation for Ring Confidential Transactions and is mandatory for all Monero transactions. An improved version of ring signatures referred to as a 'multi-layered linkable spontaneous anonymous group signature' which allows for hidden amounts, origin and destination of the transaction.
Monero, 'RingCT' (Muneropedia, 2022)
<https://www.getmonero.org/resources/moneropedia/ringCT.html>accessed 18 September 2022.

[97] [2019] EWHC 3556 (Comm); [2020] 2 All ER (Comm) 704.

[98] AA v Unknown and other (n 97) [6] (Bryan J).

> Hello [insured customer] your network was hacked and encrypted. No free decryption software is available on the web. Email us at […] to get the ransom amount. Keep our contact safe. Disclosure can lead to impossibility of decryption. Please use your company name as the email subject.[99]

In response to communication from the incident response company asking the hackers for their terms of decryption, the hackers replied in the following terms:

> Hello, to get your data back you have to pay for the decryption tool, the price is $1,200,000 (one million two hundred thousand). You have to make the payment in Bitcoins.[100]

Further negotiation lead to the first defendants lowering their demand and agreed instead to release the decryption tool on the following terms:

> as an exception we can agree on US $950K for the tool. You can send us a few encrypted files for the test decryption ((do not forget to include the corresponding _readme files as well).[101]

After the first Defendants tested several encrypted files to check if the decryption tool was working, they sent the following correspondence:

> The Bitcoin address for the payment […] When sending the payment check the USD/BTC exchange rate on bitrex.com we have to receive no less than USD 950K in Bitcoins. It takes around 40–60 minutes to get enough confirmations form [sic] the blockchain in order to validate the payment. Upon receipt we send you the tool.[102]

2.18. The ransom was transferred in Bitcoins to the hackers address by an agent of the Claimants, who also assists with the purchase and transfer of crypto currencies. The incident response company requested confirmation of receipt and expressed their hope of receiving the access tool as promised by the hackers. The tool with brief instructions was sent the following day to the incident response company. The time taken to decrypt the system varied based on the type of system and the number of files on each system. It is reported that it took 5 and 10 business days respectively to decrypt 20 servers and 1000 desktop computers.[103] Even though the insurers agreed to the payment of the ransom, further investigations were made by an employee of the insurers with the assistance of Chainalysis Inc, a blockchain investigations company who also provides

[99] Ibid [2].
[100] Ibid [4].
[101] AA v Unknown and others (n 97)[5].
[102] AA v Unknown and others (n 97) para [7].
[103] Ibid [11].

software to track the payment of cryptocurrency.[104] The investigations successfully revealed the location of the Bitcoins, 96 of which was found at an address operated by the 3rd and 4th Defendants while some was transferred to a fiat currency account. The insurers successfully made an application to the High Court for a proprietary injunction over the cryptocurrency. It was held by the court that cryptocurrencies are property as they met the four criteria of property; 'being definable, identifiable by third parties, capable in their nature of assumption by third parties and having some degree of permanence'.[105] Thus the bitcoins could be the subject of a proprietary injunction. The decision was an adoption of points made in the Legal statement on cryptoassets and smart contracts by the UK Jurisdiction Taskforce.[106] Though not a legal principle formulated in the judgment, practically the case demonstrates that insurers will not refuse to indemnify an assured for ransom paid to traditional pirates or cyber criminals solely because the ransom is to be paid in cryptocurrencies and not fiat currency. Therefore, the recoverability of the ransom paid from the insurers will still be dependent on the legality of the transaction and whether the assured complied with the policy conditions that must be met before they agree to pay a ransom.

C. Causation and Potential liabilities

2.19. Establishing causation is important for a more accurate attribution of liability and indemnification of the assured for loss or damage caused by an insured peril. Causation in marine insurance is based on the principle of proximate cause of loss. The objective of the principle is to give effect to the intention of the parties within the contract of insurance so that cover will be provided for any loss that can be fairly attributed to the operation of a covered peril.[107] *Section 55 (1)* of the *MIA 1906* provides that "… unless the policy otherwise provides, the insurer is liable for any loss proximately caused by a peril insured against'. Proximate cause of the loss does not mean the act which is last in time[108] but rather it means the dominant or real efficient cause leading

[104] ibid [12]-[13] (Bryan J).
[105] AA v Unknown and others (n 97) [55]- [61] (Bryan J); National Provincial Bank Ltd v Ainsworth [1965] 2 All ER 472, 494 (Lord Wilberforce).
[106] UK Jurisdiction Taskforce, 'Legal statement on cryptoassets and smart contracts' (November 2019) <https://technation.io/lawtech-uk-resources/#cryptoassets> accessed 18 September 2022, paras 15 and 71- 85.
[107] Wan Izatul Asma Wan Talaat, 'Causa Proxima Non Remota Spectatur: The Doctrine of Causation in the Law of Marine Insurance' (July 2003) 34 J. Mar. L. & Com. 479.
[108] *Pink v Fleming* (1890) 25 QBD 396.

naturally and reasonably to the loss.[109] *Bennett* describes the proximate cause as 'the actual infliction or the act which renders inevitable loss or damage'[110]. The assured has to prove on a balance of probabilities that the loss was caused by a peril (piracy) insured against which occurred during the period of the insurance policy.[111] Once this is established, the expectation is that the relevant insurers will reimburse the shipowner for his loss provided the assured has not breached any of his obligations under the insurance contract nor is there evidence to suggest that the loss was attributable to his wilful misconduct.[112] If the assured fails to establish causation, the insurer will not be liable to indemnify the assured for his loss. The burden of proof shifts to the insurer if he rejects the claim on the premise that the loss was caused by an excluded peril.[113] The insurer is equally responsible to prove the breach of a condition that would relieve him from liability to the assured.[114] If the policy includes a reverse burden clause, the assured must disprove the insurer's case that the loss was proximately caused by an excluded peril.[115]

2.20. As encouraged by *Lord Wright* in *Coxwold*[116], in determining the proximate cause of the loss, there should be an application of a common-sense approach of what a businessman or seafarer would take to be the cause of the loss based on the facts. With that said, if we are to view the cyber-attack as a separate incident from the pirate attack it would still be fair to reason that the dominant or efficient cause which led to the loss was the pirate attack. The reason is that malicious penetration of the navigation system on its own did not cause the loss. In fact, if the pirates did not attack and seize the Orion they would not have been in the position to demand the £10 million in bitcoin for the release of the crew and vessel. Another approach to identify the proximate cause of the loss is to consider the cyber element as a trigger to the actual loss whereas the pirate attack is the operative cause of the loss. In other words, the cyber-attack was carried out in furtherance of

[109] *Reischer v Borwick* [1894] 2 QB 548, 550; *Leyland Shipping Co Ltd v Norwich Union Fire Insurance Society Ltd* [1918] AC 350.
[110] Howard Bennett, *The Law of Marine Insurance* (2nd edn Oxford 2006) para 9.35.
[111] *Rhesa Shipping Co SA v Edmunds (The Popi M)* [1985] 1 WLR 948, 954.
[112] MIA 1906, s. 55 (2) (a)
[113] Bennett (n 110) para 7.58; Bond Air Services Ltd v Hill [1955] 2 QB 417, 427.
[114] Ibid.
[115] Bennett (n 110) para 7.58; *Bond Air Services Ltd v Hill* [1955] 2 QB 417, 427; *Spinney's (1948) Ltd v Royal Insurance Co Ltd* [1980] 1 Lloyd's Rep 406, 426.
[116] *Yorkshire Dale SS Co Ltd v Minister of War Transport, 'Coxwold'* (1942) 72 LIL Rep 1, HL, 10.

the pirate attack therefore it is only appropriate for both events to be deemed connected and to constitute a single insured event.

2.21. It is also possible to argue that the cyber-attack is the proximate cause of the loss despite the pirate attack being last in time. The rationale is, had it not been for the actions of the hackers, the Orion would have avoided the geographical area prone to piracy. It would therefore be highly improbable that the vessel and crew would have been detained by the pirates who are now demanding a ransom for their release. Similar arguments were successfully presented in *Green v Elmslie*[117], where the vessel stranded but did not sustain serious damage and was later captured. Lord Kenyon reasoned that if the vessel sailed to any other coast but that of the enemy, it would have been safe. As such the loss was caused by capture and not a peril of the seas. Conversely, if the stranding caused substantial damage to the vessel and then seized for example in *Hahn v Corbett*[118], the loss would be caused by perils of the seas. The better option may be to consider the cyber and the pirate attack as proximate causes of the loss since both are 'approximately equal in effectiveness as such it is impossible to label one as more dominant than the other'.[119] That is, had it not been for the combination of events that is the taking of the vessel and crew, the ransom demand would not have occurred. Arguably, if either was absent the loss would not have occurred. The general principle as it relates to concurrent causes of loss would be applicable. Accordingly, if the insurance policy purchased by the shipowners covers piracy and seizure but is silent on the cyber as a peril then the assured would be allowed to recover for their loss.[120] Conversely if cyber risk is expressly excluded from the policy, then the assured would not be able to recover for his losses.[121]

2.22. The more challenging aspect is to determine the motive behind the attack. The facts are sparse but there is no evidence to suggest that the pirates who attacked and captured the crew and vessel had a political motive. Conversely, what if the hackers had a political motive whereas the

[117] *Green v Elmslie* 170 E.R. 156; (1794) Peake 279.
[118] *Hahn v Corbett* 130 E.R. 285; (1824) 2 Bing. 205.
[119] *Wayne Tank and Pump Co Ltd v Employers Liability Insurance Corporation* [1974] QB 57 (CA) 68-69.
[120] *'Miss Jay Jay'* [1987] 1 Lloyd's Rep 32 (CA) 37.
[121] *Samuel v Dumas* (1924) 18 LIL Rep 211, 222; *Wayne Tank and Pump Co Ltd v Employers Liability Insurance Corporation* [1974] QB 57 (CA) 75.

pirates' motive was merely for personal gain? The answer to this question would depend on the proximate cause of the loss. Alternatively, as was decided in *Banque Monetca & Carystuiaki v Motor Union Insurance Co Ltd*, where there was evidence of both personal gain and political motive behind the attack, in determining whether the attack amounted to piracy, the dominant motive will be the deciding factor. In this case, the dominant motive is to secure the ransom payment, any political motivation would be speculative and not enough to change the character of the attack. While attribution of liability is not a guaranteed, genuine attempts must be made to determine the motive(s) behind cyber-attacks. Such efforts ought to include forensic investigation to trace the origin of the attack. If the origin of the attack is established, it becomes easier to categorize whether the attack was for personal or political gain. If the region or the group responsible for the attack is identified, the next step would be to ascertain whether the region or group is associated with a political ideology which conflicts with that of the victim or is notorious to investigative task forces for committing cyber-attacks. Though very rare, the motive behind a cyber-attack is easily established when a group or individual declares they are responsible for the attack or had publicly declared their intention to carry out attacks. This is similar to the declarations made by terrorist groups such as al Quaeda or Boko Haram stating they are responsible for terrorist attacks. The modus operandi of certain groups if studied over a period would also be a good indication of the motive of hackers. However, it cannot be denied that the cyber element complicates any attempt to accurately place a motive behind the attack as it is difficult but not impossible to know the identity of the perpetrators and their geographical location. The purpose for which the ransom money is to be expended can also help to determine or alter the character of the attack. That is, if the money is to support a political group or terrorist organization then the character of the attack would change from piracy to a war risks or terrorism. If such are the circumstances behind the attack, issues as to the legality of the ransom payment will be brought into contention.[122]

2.23. If the conclusion that these facts satisfy the requirement of piracy is incorrect, could this then be considered as seizure and if so, what are the insurance implications? The pirates were said

[122] Terrorism Act 2000, s. 15(3). Ransom payments are not illegal under English law provided they are not paid to or have any association with terrorist groups.

to have captured Orion; however, the facts indicate that a seizure has occurred. Capture is given a restricted interpretation unlike seizure. The distinction between capture and seizure was made by Lord Fitzerald in *Cory & Sons v Burr* where he said "that capture and seizure do not mean the same thing. Capture would seem to include every act of seizing or taking by an enemy or belligerent whereas seizure is a wider term and includes every act of taking forcible possession either lawfully or by an overpowering force."[123] For seizure, the existence of belligerent acts is not necessary nor is the intention that the owner will be disposed permanently of his possession.[124] Since the pirates intention was not to permanently deprive the shipowners of their vessel nor could they be considered a belligerent enemy, it is more appropriate to categorize their action as seizure. Therefore, there was piracy accompanied by seizure against the Orion and crew.

2.24. Originally the combination of events, that is, the piracy and seizure though possible, was frowned upon by insurers. This was evident in *Kleinworth v Shephard*[125] where the vessel was insured against piracy and 'warranted free from capture and seizure and the consequences thereat'. The passengers attacked the crew and seized the vessel. It was held that despite piracy being a covered loss, since there was also seizure which is an excluded peril, the insurers were not liable and so the assured could not recover for their loss. This is a harsh decision particularly because pirates sometimes engage in seizures and captures simultaneously thus it is irrational for the assured to be denied cover because the pirates did more than just rob indiscriminately but for example in this case, decided to seize the vessel and hold the crew hostage until a ransom is paid. The Lloyds market realized the disadvantage to the assured and has mollified the effect of such decisions by incorporating clause 24.2 and 21.2 of ITCH (95) and IVCH (95) respectively both of which clarifies that the exclusion of seizure from marine policies does not include piracy.[126] This

[123] (1883) 8 App Cas 393, 405; *Forestal Land, Timber and Railways Co Ltd v Rickards (The Minden)* [1940] 4 All ER 96, 109 Hilbery J expressed similar views 'capture is taking by the enemy as prize in time of open war with intent to deprive the owners of their property in the goods.'

[124] Bennett (n 110); *Johnson & Co v Hogg* (1883) 10 QBD 432.

[125] (1859) 1 E & E 447.

[126] ITCH (95) 24.2; IVCH (95) 21.2: In no case shall this insurance cover loss damage liability or expense caused by capture seizure arrest restraint or detainment (barratry and piracy excepted), and the consequences thereof or any attempt thereat.

means that even though the act of the pirates might also amount to seizure, it does not preclude cover to the assured for losses arising from the pirate attack.[127]

2.25. Since piracy is determined to be the proximate cause of the loss and no legality concerns were raised, there are three insurance implications for the assured shipowner; first, the assured may have insurance coverage through his original marine insurance policy where cyber risk has not been explicitly excluded, secondly the assured is without cover under his traditional marine insurance policies due to the incorporation of an exclusion clause and thirdly though very rare, the assured may be protected from this loss through a cyber insurance policy specifically designed to cover marine losses caused by a cyber-attack. Each possibility will be assessed in alternate order.

II. Marine Insurance: Is Silence Acceptance?

A. Non -exclusion of cyber risks in Marine Insurance

2.26. Piracy is covered under marine hull and or all-risk cargo policies. However, in the past, piracy was at times under the umbrella of marine insurers and other times under war risk policies. This means that even though the standard hull policies cover loss or damage from piracy, some marine insurers exclude piracy from their cover forcing shipowners to purchase such protection elsewhere, for example under a war risks policy for additional premium or a kidnap and ransom policy. However, the main focus here is to discuss the cyber pirate attack under marine hull policies. The Institute Time Clauses Hull and the Institute Voyage Clauses Hull (1995) both provide cover for piracy, however at the time of their writing, it was not within the contemplation of the drafters and insurance practitioners that cyber risks would become a peril that could cause harm to vessels and other marine facilities. Consequently, loss or damage caused from a cyber-attack or incident is not listed as a peril covered or excluded under any of the Hull Institute clauses, even the most recent version (2003). A closer look at the scenario will indicate that the navigation system of Orion was penetrated by a malicious virus which was used to reroute the vessel to a strategic location for the pirates to capture the vessel and crew and demand a ransom. Since the proximate cause of the loss was determined to be piracy and there is no exclusion of cyber risks,

[127] Baris Soyer, *Marine Insurance Fraud* (Informa Law 2014) 206.

the assured would be covered under clause 6.1.5 and 4.1.5 of the Institute Time and Voyage Clauses - Hull respectively, provided there was loss or damage caused to the vessel. Moreover, in paragraph 21.2 of IVCH (95) and 24.2 of ITCH (95) capture, seizure, arrest or restraint and the consequences thereof are excluded but piracy and barratry are excepted, a validation that piracy will be covered by the hull insurers. Also, the International Hull Clauses 2003 in clause 2.1.5 covers loss or damage to the subject matter insured caused by piracy. Alternately, if both the cyber and pirate attacks are accepted as concurrent causes of the loss and there is no exclusion of the cyber risks, the insurers will be liable to indemnify the assured for their loss.[128] The hull insurers would be expected to cover the 'ransom' paid to the cyber criminals even though the circumstances leading to the peril was unforeseeable by the parties at the time of contracting. The pertinent point is that the cyber risk has not been excluded and unless the insurers successfully present a defence, the assured is to be reimbursed for the expenses incurred to protect the vessel. As it relates to cargo loss or damaged from the cyber piracy attack, the cargo loss caused by piracy will only be covered if ICC (A) all risks policy is added to the assured cargo insurance and there is no exclusion of cyber risks. ICC (A) offers protection against all perils provided it's not explicitly excluded in the policy.[129] There is no protection for loss caused by piracy in ICC (B)[130] and ICC (C)[131] as they are named risks and piracy is not one of the insured perils listed in the policy.

2.27. In the marine insurance market, there are policies designed specifically to address risks from piracy, which differs from traditional K&R policies in that they protect not only the persons onboard but also the vessel.[132] A principal element of this policy is its focus on marine piracy as a peril and effective crisis management which include the services of negotiation consultants and a public relations team to control and attempt to remedy the reputational damage which the owners of Orion are likely to experience. Another significant feature of policy is that the assured will be reimbursed the ransom paid to the pirates and that the sum will be insured while in transit to the

[128] *Instruments Ltd v Northern Star Insurance Co. Ltd (Miss Jay Jay*) [1987] 1 Lloyd's Rep 32, 36.
[129] Institute Cargo Clauses (A) (1/1/82).
[130] Institute Cargo Clauses (B))1/1/82).
[131] Institute Cargo Clauses (C)(1/1/82).
[132] Beazley Insurer, 'Marine Piracy'
(2022) < https://www.beazley.com/london_market/marine/marine_piracy.html>accessed 18 September 2022.

chosen location. Since the hackers and pirates in the scenario requested payment through electronic methods, it is not clear whether similar insurance will be offered against electronic fraud just in case the ransom is intercepted or stolen before it is paid to the hackers and pirates. It would not be commercially prudent to restrict a term of the policy to only physical transactions when systems are mainly operated through online electronic methods and at time when bitcoin and other electronic payments are becoming more acceptable within the marine sector. Furthermore, additional expenses which could include the sue and labour or general average expenses incurred to minimize the loss to the assured and the fees for legal services are recoverable. There is also protection against physical damage, personal accident and it is optional for the assured to include loss of hire coverage. The limit for piracy begins at US$15 million which can increase upon the request of the assured. This policy can either be a compliment to other insurance packages or stand as a policy on its own. The insurers suggest there could be a combined war and marine piracy coverage with limits of up to US$ 75 million. This policy coverage would have been ideal for a shipowner who is at risk of a pirate attack. The only problem here is the sub-limits for marine is below the costs incurred by the assured, therefore he would be need to a seek the assistance of his P&I insurer to cover the difference.

2.28. Exposure to silent cyber risks is an issue marine insurers would have encountered whose policies were written before 1 January 2020.[133] Even prior to that date, cyber awareness gradually became a priority for all stakeholders in the marine sector so that considerable efforts were being made to reduce unintended exposure to cyber risks. Today, it is unlikely to find a marine policy that is non-affirmative on cyber risks, however the discussion is still relevant for cases which may have occurred under older policies that are not yet settled. Accordingly, in the next section, the assured's alternative arguments to recover from their insurers the ransom amount paid to the cyber criminals will be discussed.

[133] Lloyds, 'Providing clarity for Lloyd's customers on coverage for cyber exposures (Market Bulletin Y5258)' (4 July 2019) <https://www.lloyds.com/news-and-insights/market-communications/market-bulletins/?Query=Y5258&Filters=%5B%5D&OrderBy=&Page=1&StartDate=&EndDate=&Type=MarketBulletin&DateChanged=false&HideFields=> accessed 18 September 2022.

B. Alternative claims

a. Constructive total loss

2.29. A claim for constructive total loss would be futile in the present case as there is insufficient evidence that the vessel and cargo were abandoned, and that actual total loss was unavoidable.[134] The tendency has been that vessels captured by pirates where a ransom demand has been made is in most instances released once the ransom has been paid to the pirates. Unless the assured can prove otherwise, a claim for constructive total loss would be difficult. The modus operandi of Somali pirates was examined in *The Bunga Melati Dua*[135] and the observation made by David Steel J in relation to other vessels was that 'no cargoes had actually been lost and the evidence suggest that ship cargoes were likely to be released after 6 to 8 weeks.' Another case that illustrates the recovery prospects of seized assets following the payment of a ransom is *The MV Polar*[136]. While on a voyage from St Petersburg to Singapore, *the MV Polar* was held by Somali pirates for 10 months, from the 30 October 2010 and released on 26 August 2011 following the payment of US$ 7, 700, 000. Some of the cargo was removed during the seizure of the vessel but the balance was delivered to Singapore. The status quo has not changed much since that decision was made, so it is highly probable that the crew and vessel along with any cargo onboard the Orion would be released to the shipowners once the ransom transfer has been confirmed.

2.30. The statistics are just as positive for ransomwares and the recovery of data after the ransom has been paid. In 2018, 49% of companies who were victims to a ransomware attack paid the ransom and recovered their data whereas in 2021, 72% of the companies recovered their data after a ransomware attack.[137] There is no basis for any contention that the vessel and cargo was abandoned by the shipowners, this would be a difficult decision to make considering that the lives of crew members are also dependent on the successful negotiation between the shipowners and the

---

[134] Marine Insurance Act 1906, s. 60 (1).
[135] [2010] 1 Lloyd's Rep 509 [1.076].
[136] *Herculito Maritime Limited and others v Gunvor International BV and others (The Polar)* [2020] EWHC 3318 (Comm); [2021] 1 Lloyd's Rep. 150 [3].
[137] CyberEdge, '2021 Cyberthreat Defense Report' (2021) 3 <https://www.imperva.com/resources/resource-library/reports/2021-cyberthreat-defense-report-report-ty?lang=EN&asset_id=4568> accessed 18 September 2022.

pirate / hackers who have taken control of the ship. The shipowners were actively negotiating with the pirates, those actions suggest the shipowners had reasonable belief that their vessel, crew and cargo would be returned so there is no argument or evidence of abandonment on the part of the assured shipowner. In any event, if the shipowners could establish, they would be permanently deprived of the insured vessel, there is no legal principle which would prevent the shipowners from claiming that the ransom paid was to prevent constructive total loss. Rather than a claim for constructive total loss, in practice, this would usually be made as a sue and labour claim, which will be discussed next. The situation reverses if the cyber-attack led to a collision which caused so much damage that it is not economically feasible to repair the vessel or alternatively if the pirates were more interested in keeping the vessel and cargo rather than a request for a ransom. The involvement of the hackers and malware would not prevent a successful claim for constructive total loss, provided there is no exclusion of cyber risk.

b. Sue and labour expenses

2.31. On another note, it is possible that a claim could be made that the ransom paid by the ship owners is to be treated as a sue and labour expenses[138] as provided for under section 78 (4) of the *MIA 1906* and clause 11.1, 11.2 and 9.1, 9.2 respectively of the ITCH and IVCH 1995. By these provisions, 'the assured their servants and agents in any cause of loss or misfortune has an obligation to take such measures as may be reasonable to avert or minimize a loss which would be recoverable under the insurance.' Part two (2) of clause declares that 'for the efforts by the assured and their servants and agents, the underwriter will contribute to charges properly and reasonably incurred.' *Phillips J in Royal Boskalis* when referring to the ransom paid to secure the release of the vessel concluded that

> the terms in section 78 (4) are wide enough on their natural meaning to embrace expenditure necessary to procure the release of a vessel that has been seized…If that is right, then it would be strange indeed if such expenditure did not fall within the sue and labour clause. In my judgement the assumption of the editors of Arnould that payment of a ransom, if not itself illegal, is recoverable as an expense of suing and laboring is well founded.[139]

[138] *Royal Boskalis Westminster NV v Mountain* [1999] QB 674, 717 'The payment of a ransom in order to secure the release of property insured against seizure is an example of a sue and labour expense.'
[139] Ibid, 720.

While the *MIA 1906* stops at the general obligation to take such measures as may be reasonable to avert or minimize a loss, insurance contracts such as the Institute Hull Clauses limits this duty to a 'loss which would be recoverable under this insurance'. This is important as the latter explicitly provides that if the sue and labour expenses were incurred to prevent a loss excluded under the contract, for example to prevent the loss of lives (IVCH (95) 6.4.4, the insurers would not be under any duty to reimburse the assured.[140] Though not expressly provided, the same principle is implied when interpreting *s. 78 (4) MIA 1906*. While the hull insurers would not have a right to claim damages if the assured failed to mitigate their loss[141], it is the right of the insurer to limit their liability to the point and extent to which the latter can prove aggravated losses due to the omission or negligence of the assured.[142]

2.32. An interesting point is that the decision to pay the ransom to the pirates / cyber hackers may not be categorized as a sue and labour event by insurers if they successfully argue cyber is not a peril that is covered by the insurance contract, or the owners failed to exercise the necessary due diligence to ensure their systems maintain adequate cyber hygiene. The first part of this counter argument will be rejected as there is no cyber exclusion endorsed on the policy. Furthermore, at this stage where guidelines have been issued by both the government and the industry[143] encouraging stakeholders to manage cyber risk, insurers cannot continue to reject claims caused by a cyber threat or attack solely on the basis that it was not a named peril. As aforementioned, The PRA Supervisory Statement (SS4/17) on cyber insurance underwriting recommended that insurers 'state whether cover is provided for cyber risks or not, adjust premium accordingly, introduce robust wording exclusions and or specific limits of cover'; while Lloyds Bulletin Y5258 made it mandatory for insurers to exclude or affirm cyber cover for all policies incepted on or after 01 January 2020.[144]

---

[140] F.D. Rose, 'Failure to Sue and Labour' Journal of Business Law 1990.
[141] Paul Todd, Fraud & Piracy (2nd edn, Informa 2010).
[142] *State of the Netherlands v Youell [*1997[2 Lloyd's Rep 440, 458.
[143] Bimco and others, 'The Guidelines on Cyber Security Onboard Ships: Version 4' (Annex 4, 2020) <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships> accessed 18 September 2022.
[144] See (n 27), (n 28).

2.33. The point was made above that sue and labour expenses will only be reimbursed if they were incurred to minimize or prevent a loss that is covered under the insurance contract. The example given to prevent the loss of life is excluded under hull policies, so it is questionable if the ship owners would have been reimbursed for sue and labour expenses where part of the ransom contributed to saving the lives of the crew members who were detained by the pirates. The presumption would be to apply the principles from cases such as *Miss Jay Jay*[145], which held that there will be no insurance coverage if there are two proximate causes of the loss, one of which is excluded. However, the applicable principle is not the same where the expenditure incurred is directed to two objectives one of which is to minimize or avert a loss insured and another which is outside the limits of the policy. The rule is stated in the *B Atlantic* by Flaux J:

> where expenses are incurred both for the purpose of extricating the vessel from the insured peril and for some other purpose which is not sue and labour (here the defence of the crew) there is no principled basis for apportioning the expenses between those purpose so they are all to be properly regarded as sue and labour expense… it is only if the insurers can demonstrate that the relevant expenditure was incurred solely for the other purpose that the expenditure will not be recoverable as sue and labour [146]

Another supporting authority is to be found once more in the decision of Philips LJ in *Royal Boskalis* where he addressed the issue of crew at risk when a ransom payment is demanded**.** Rix J at first instance had reduced the award to the assured by 50% on the ground that the losses were incurred not just to release the vessel but also the crew. At the Court of Appeal, Phillips LJ rejected this contention and held that:

> it has never been the law that liability under a sue and labour clause should be reduced because the exertions was motivated in part by a desire to save lives. Provided that expenses can reasonably be said to have incurred for the preservation of the property, it does not seem to me either sound in principle or desirable that the assured should be penalized if they were sufficiently concerned for lives at risk to have been concerned to save not only their property but those lives.[147]

2.34. Therefore, based on this reasoning the fact that the ransom was paid to also release the crew will not preclude the ransom and other expenses from being categorized as sue and labour

---

[145] *'Miss Jay Jay'* [1987] 1 Lloyd's Rep 32 (CA); *Samuel v Dumas* (1924) 18 LIL Rep 211, 222.; *Wayne Tank and Pump Co Ltd v Employers Liability Insurance Corporation* [1974] QB 57 (CA) 75.

[146] [2015] 1 Lloyds Rep. 117, para 346.

[147] *Royal Boskalis Westminster NV v Mountain* [1999] QB 674, 739.

expenses which can be claimed fully from the hull insurers provided, they were reasonably incurred for the preservation of the vessel and cargo. There is the view that in some cases 'an apportionment of the expenses should be acceptable otherwise hull insurers will incur a risk which they did not intend to bear'[148], akin to the impact of the cyber risks in this scenario on insurers liability. It was proposed that in situations where the ransom was primarily to save the vessel or to save the crew where they are separated from the vessel, apportionment should be allowed.[149] While the point is clear, it is suggested that Phillips LJ could not have intended that hull insurers would pay for expenses incurred to save the crew because hull insurance policies specifically exclude such risk. This is a risk that would be borne by the shipowners P&I club or K&R insurers. Phillips LJ discussion focused on cargo vessels where the property onboard including preservation of the vessel was the main motivation while the release of the crew was merely incidental to those expenses being incurred. The pirates in this scenario did not hold the crew hostage and demand a ransom, they instead took control of the vessel and had in their possession whatever cargo onboard. If they had taken the crew and had no interest in the vessel and cargo, then it is understandable why any expense incurred to release the crew could not be a bill that should be the sole responsibility of hull insurers but should instead be apportioned among the insurers. A similar reasoning was applied to the interpretation of the facts of *m/ v Leopard* whose crew was captured in January 2011 but was not released until 2013. The pirates found it challenging to take control of the vessel due to a malfunction of the propulsion. Marsh insurers expressed their view that because the H & M and or War Risk Insurers had no 'financial interest in the wellbeing of the crew, it would be highly unlikely that the insurers would willing reimburse any payment made by the shipowners towards the release of the crew alone.'[150] In fact, the recommended approach is that ransom paid should be claimed as sue and labour expenses when the vessel is on a ballast trip and unchartered. Otherwise, the better option is to claim the ransom paid as general average[151], which takes us to the discussion below.

[148] Todd (n 141) para 1.099 – 1.100.
[149] Ibid.
[150] Marsh, 'Piracy – Insurance Implications' (2011)
< https://static.mycoracle.com/igpi_website/media/article_attachments/Marsh%20Piracy%20implications.pdf> accessed 18 September 2022.
[151] Ibid.

c. General average contributions

2.35. According to section 78(2) of *MIA 1906*, 'general average contributions and salvage costs cannot fit under the sue and labour clause, therefore if the Orion is transporting cargo, the most appropriate option for the shipowner if he wishes to recover some of the expenses from other interests would be through general average claims. Ideally, the shipowner will recover the sue and labour expenses from his hull insurer who in turn will be subrogated in respect of the contributions from other third-party interests in the subject matter insured[152]. To be more specific, where cargo is involved, the hull insurer may seek contribution from cargo insurers if the contract of insurance includes a corresponding sue and labour clause such as clause 16 of ICC (A) 1982.[153] Therefore, an alternative option for the shipowner is to seek to recover his contributions through general average claims.

2.36. Section 66 (2) of the *MIA 1906* defines 'a general average act as any extraordinary sacrifice or expenditure voluntarily and reasonably made or incurred in the time of peril for the purpose of preserving the property imperilled in the common adventure.' Both the sue and labour and the general average clause require that the expenses incurred, or the sacrifices made be reasonable. The circumstances which led to the detainment of the Orion and its crew would cause any objective person to agree that the payment of the ransom was the best, most efficient and reasonable option that was available to preserve the vessel, its cargo and crew members. The conversation as to whether the ransom amount paid by the shipowners is reasonable / adequate was left open in the leading judgement of Lord Neuberger in *Longchamp*[154], as he thought it unnecessary to decide upon that issue 'in order to justify the contention that the negotiation period expenses were allowable under Rule F of the York Antwerp Rules'. He made the very cogent point that what should be of concern is the nature and not the quantum of the ransom since it will be difficult for shipowners to ignore a ransom demand or for cargo interests to refuse contribution simply because

[152] MIA 1906, s. 79.

[153] Baris Soyer, *Marine Insurance Fraud* (Informa Law 2014), 217.

[154] *Mitsui and Co Ltd and others v Beteiligungsgesellschaft LPG Tankerflotte MBH and Co KG and another; The Longchamp* [2018] 1 All ER 545.

the sum demanded by the pirates is 'unreasonable'. In fact, the appropriate conversation as Lord Neuberger has proposed should not be about the reasonableness of the ransom.

2.37. Lord Mance contributed to the conversation in his dissenting judgment where he stated;

> if the safest, most timely and effective means to secure the release of the ship & crew was to pay a ransom, it follows that the most safe, timely means of so doing is to pay it as soon as possible.[155]

He further commented that while the general practice in dealing with Somali pirates is to negotiate to lower the ransom, the decision to pay straight away is not in itself unreasonable, as it is meant to avert the real danger to the vessel, cargo and crew as quickly and effectively as possible.[156] Similar arguments are transferable to these facts, therefore the absence of a prolonged negotiation between the pirates and the shipowners cannot be the foundation on which the cargo interests refuse to contribute to the general average sacrifice. The objective is to save the crew members, protect the cargo and vessel and if paying the ransom forthwith is the best option to avert these losses, the payment is 'reasonable' to satisfy the requirements under the general average clause. The ransom is an additional expense incurred in place of the otherwise inexorable expenses that would have been allowable as general average[157] for example value of the cargo damaged or lost, wages and maintenance of crew, actual or constructive total loss of the vessel and salvage expenditures including efforts to prevent or minimise environmental damage, personal injury and death.

2.38. In any event, it is to be noted as well that the shipowners in this scenario contend with a bigger threat than what Somali pirates pose. While it is possible to predict and prepare for example, the actions of Somali pirates, it is difficult to assess how much damage the hackers have done and or willing to create and the level of control they have over the vessel, cargo and crew. Therefore, it is not implausible for the insurers to quickly assess that it is in the assured's best interest to transfer the ransom to the pirates. The shipowners should be aware of the modern tactics of pirates

[155] Ibid 565-566.
[156] Ibid.
[157] York Antwerp Rule 2016, Rule F.

and must also be cognizant that the vessel and crew are usually released after negotiating with the pirates and confirmed delivery / transfer of the ransom. A genuine concern with the payment of the ransom is that while the crew and vessel may have been released, now that a cyber element is involved, there is no guarantee that Orion's system will be restored to its original state. The cyber risks will not affect a sue and labour or general average claim where the policy is silent on cyber as a peril. As there is no cyber exclusion clause, the hull insurers may again be expected to reimburse the assured for its GPS and any other computer hardware and systems which have been damaged or is malfunctioning due to the attack. The *MV Polar* decision confirms that owners may seek contribution in general average from bill of lading holders in respect of the ransom payments made to the Somali pirates to release the vessel.[158] The sum was paid by the K&R and War risks insurers who then seek contribution for general average which cargo owners rejected on the basis that the bill of lading incorporated the charterparty under which the only remedy for the shipowner was to recover the ransom paid from their K&R and war risks insurers. The arguments failed and the shipowners were allowed to recover contribution from the cargo insurers so that each party with an interest in the voyage will share the risks. There would need to be a clearly expressed clause stating that the owner has agreed to waive their right to a contribution in general average for the ransom paid from the cargo interest. The foregoing illustrates that ransom payment made by the shipowners to secure the release of a vessel can be either a sue and labour expenses or alternatively general average contribution or sacrifice. Another important point from *the Longchamp* is that the fees incurred to negotiate with the pirates are recoverable under sue and labour expenses.[159]

2.39. Rule D of the York Antwerp Rules provides a defence for the cargo interest if they were to successfully argue that the general average sacrifice, in this case the ransom payment and negotiation cost were incurred due to the breach of the contract of carriage. They may insist that the Orion was unseaworthy because the shipowners did not ensure the vessel was cyber resilient or at the very least kept the vessel IT systems and GPS systems updated in line with the

[158] *Herculito Maritime Limited and others v Gunvor International BV and others* (The Polar) [2020] EWHC 3318 (Comm); [2021] 1 Lloyd's Rep. 150 [104], [110] – [114].
[159] *The Longchamp* [2018] 1 All ER 545.

recommended best practices[160]. If they can prove this, cargo interest will have a defence to the contribution request and the shipowner's only option would be to try to recover the ransom and other P&I type expenses from their P & I club.

C. P& I Club and Cyber Piracy

2.40. There is no general exclusion of piracy from P&I insurance therefore third party liabilities that are usually insured by the Club will remain covered when arising from a pirate attack provided that weapons of war and terrorism exclusions are not triggered.[161] Therefore such liabilities do not usually include loss or damage to the hull of the vessel arising from piracy. Furthermore, ransoms are not covered because P&I clubs will only cover liabilities from an incident for which the shipowner is legally or contractually responsible. As mentioned earlier there is no evidence of any weapon of war[162] being utilized by the pirates and any link to terrorists or their affiliates have been dismissed. The act of the pirates and the cyber hackers was for personal gain unrelated to a political group or government. P&I clubs have stated that if no other insurer is willing to cover a ransom payment, it is possible this might be recoverable from P &I clubs at the discretion of the boards under sue and labour or under the omnibus provision which would be a contribution to the

[160] Bimco and others, 'The Guidelines on Cyber Security Onboard Ships: Version 4' (Annex 4, 2020) <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships>accessed 18 September 2022; BIMCO and others, 'Global Counter Piracy Guidance for Companies, Masters and Seafarers: High Resolution' (Witherby Publishing, June 2018) <https://www.maritimeglobalsecurity.org/media/1040/global-counter-piracy-guidance-bmp_high_01-04-19.pdf> accessed 18 September 2022; BIMCO and others, 'BMP5 Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea: High Resolution' (Version 5, Witherby Publishing June 2018) <https://www.maritimeglobalsecurity.org/media/1038/bmp5-high_res.pdf > accessed 18 September 2022; IMO, 'Piracy and Armed Robbery Against Ships: Guidance to shipowners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships' (MSC.1/Circ.1334 23 June 2009) <https://www.maritimeglobalsecurity.org/media/1008/c-users-jpl-onedrive-bimco-desktop-msc1-circ1334.pdf > accessed 18 September 2022; IMO, 'Revised Interim Guidance to Shipowners, Ship Operators and Shipmasters on the Use of Privately Contracted Armed Security Personnel on Board Ships in the High Risk Area' (MSC.1/Circ.1405/Rev.2 25 May 2012) <https://www.maritimeglobalsecurity.org/media/1009/c-users-jpl-onedrive-bimco-desktop-msc1-circ1405-rev2.pdf > accessed 18 September 2022.

[161] IG P&I, 'Revised Piracy – FAQs: Revised December 2019 < https://www.igpandi.org/article/piracy-faqs-revised-december-2019> accessed 18 September 2022.

[162] Weapons of war are mines, torpedoes, bombs, rockets, shells and explosives. Therefore, the use of regular guns and rifles often used by pirates will not trigger the weapons of war exclusion.

shipowner's H&M cover.[163] Consequently, though P&I Clubs are not keen to cover ransom paid by their members to pirates and cybercriminals and have no legal obligation to do so, P&I may exercise their discretion and reimburse the payment, though it is unknown how often this is done.[164] Some Clubs have expressed their position in their rules. The London P&I Club Rules 2022 in clause 9.27.3.2 provides that losses, costs and expenses relating to ransom will not be recoverable under their sue and labour and legal costs ensuring clause unless and to the extent the Member's Committee in its discretion decides otherwise.[165] Rule 5E (b) of the UK P&I 2002 rules demonstrates the reluctance of Clubs to cover ransom:

> Ransom shall not be recoverable unless and to the extent that the Members' Committee in its discretion shall otherwise decide. Note: when deciding whether to exercise its discretion, the Committee will consider the merits of each case individually including but not limited to whether the Owner had taken such precautions as appear to the Committee to be reasonable to avoid the event that gave rise to the ransom.[166]

One consideration of the Members' Committee would be whether the shipowners had exercised their due diligence to ensure that the vessel is cyber resilient / maintain its cyber hygiene before they started the voyage. This assessment will be based on government and industry guidelines including the SOLAS ISPS requirement, IMO Resolution MSC 428/98, national cyber security initiative where businesses are encouraged to gain cyber essential certification and implement BIMCO guidelines on how to manage cyber risk within the maritime sector. The shipowners must ensure the vessel is classed by an approved classification society and comply with all statutory requirements relating to safe operation and security and management of the ship and maintain the relevant statutory certificates from their flag state. Alternatively, P&I clubs may exercise their discretion to reimburse shipowners for ransom when it is unrecoverable under their hull or war risks policy because the assessed sound value of the vessel for general average contribution is more

[163] P&I, 'Revised Piracy – FAQs: Revised December 2019' <https://www.igpandi.org/article/piracy-faqs-revised-december-2019> accessed 18 September 2022.
[164] Baris Soyer, *Marine Insurance Fraud* (Informa Law 2014) 217.
[165] The London P&I Club, 'Class 5: The Protecting and Indemnity Rule 2022/ 2023' (2022) <https://www.londonpandi.com/documents/the-london-club-pplusi-rules-class-5-2022-2023/> accessed 18 September 2022.
[166] UK P&I, 'Rules 2022' (2022) <https://www.ukpandi.com/news-and-resources/rulebook-2022?chapter=conditions+exceptions+and+limitations> accessed 18 September 2022.

than the vessel's insured value. This is said to be one of the few ways in which P&I clubs will reimburse shipowners for ransom paid to pirates and now by extension cyber criminals.[167]

2.41. As it relates to cargo insurance and general average contribution, P&I insurers may reimburse members for cargo contribution which they would be entitled but which is irrecoverable due to a shipowner's breach of the contract of carriage, provided the breach does not also affect club cover.[168] Similarly if as in this case, there is hijacking of the vessel by pirates and the shipowner cannot recover the ransom due to unseaworthiness arising from poor cyber risk management, the shipowner might be able to recover his general average contribution from his P& I club. Since the contract between the shipowners and P&I clubs should be treated as a time policy[169], s. 39 (5) applies so there is no implied warranty of seaworthiness in the P&I contract however the insurer will be discharged of liability to the shipowner if he knowingly sends the vessel to sea in an unseaworthy state and a loss emerges as a result. Generally, However, with the amendments under the *IA 2015*, the insurer is no longer automatically discharged from his liabilities due to a breach of a warranty.[170] If the insurer did not exercise his option to contract out of section 10,[171] the insurance contract will be suspended until the breach, if possible has been remedied. The remedy for a breach of a warranty under the insurance contract can be found in Schedule 1 Part 1 where a distinction has been made between qualifying breach which was deliberate or reckless and those that are neither reckless or deliberate. There is no evidence to conclude that the shipowners or charterers were deliberate or reckless in the maintenance of their

[167] Steven J Hazelwood and David Semark, *P.& I Clubs Law and Practice* (4th ed, Informa Law 2010) 10-209; Gard, 'P&I Club Rules 2022: Rule 41(b)' (2022) <https://www.gard.no/web/publications/document/chapter?p_subdoc_id=1034258&p_document_id=781871> accessed 18 September 2022.

[168] Ibid 10-206; Gard P&I Club Rules 2002: Rule 41(a).

[169] Baris Soyer, *Warranties in Marine Insurance* (3rd edn, Informa Law 2017) para 3.90; Compania Maritime San Basilo SA v Oceanus Mutual Undertaking Association (Bermuda) Ltd (The Eurysthenes) [1977] 1 QB 49. P&I clubs may exclude the application of s. 39 (5) but 'express, pertinent and apposite language is required to contract out of s.39(5)'. For voyage policies there is an implied warranty of seaworthiness, s. 39 (1) MIA 1906. Where there is a carriage of goods contract and the Hague Visby Rules 1968 are incorporated, Article III (1) (a) places a duty on the carrier before and at the beginning of the voyage to exercise due diligence to make the ship seaworthy'.

[170] IA 2015, s. 10 (1).

[171] IA 2015, s. 16.

IT and GPS operating systems so the insurer will not have the right to avoid the contract and refuse all claims without an obligation to return the premium paid under the contract.[172]

2.42. On the contrary, since the assured shipowner have not been adjudged as reckless or having deliberately contributed to their loss the insurer may avoid the contract and refuse all claims but must return the premium paid. This would be the chain of events if the insurer would not have entered the contract on any other terms in the absence of the qualifying breach. It is widely accepted that a hull insurer would not enter a contract with an assured with the knowledge that the vessel is unseaworthy as this would increase the probability of losses to the assured which the insurer would be expected to reimburse. The element of fortuity would be lacking which is an essential component for marine insurance contracts. Under such conditions the options where the insurer would have entered the contract but on different terms or where he would have charged a higher premium on the same or on a variation of terms is irrelevant since it is an implied term at the commencement of a voyage contract for the vessel to be seaworthy.

2.43. The extent to which an assured will be penalized for his knowledge of the cyber vulnerabilities of his vessel is yet to be tested, however it is fair to reason that the assured will not be expected to personally be an expert in cybersecurity but will be expected to have the knowledge of his IT personnel and maintain his systems based on the best practices as recommended by specialist within the industry, the government and flag states. If the insurer exercises his option under s.16 of the *IA 2015* to contract out of section 10 so that each warranty in the contract of insurance must be strictly complied with, the default position under section 17 of the *MIA 1906* will be reinstated so that the insurer will be discharged of liability from the date of the breach even if the breach is subsequently remedied.[173] However, the transparency rules in section 17 of *IA 2015* requires the insurer to bring such unfavourable terms to the attention of the assured or his

[172] IA 2015, Schedule 1 part 1 (2a and 2b).

[173] Britannia P&I, 'Additional Insurances Policy Year 2021 /22: Clause 5.2' (Version 2.00 (February 2021). <https://britanniapandi.com/wp-content/uploads/2021/02/Additional-Insurances-2021.pdf> accessed 18 September 2022. Another example of this Clause provides; "Section 10 of the Act is excluded. As a result, all warranties in the contract of insurance must be strictly complied with and if the Assured or any party afforded the benefit of cover by the Association fails to comply with any warranty the Association shall be discharged from liability from the date of the breach, regardless of whether the breach is subsequently remedied."

agent before the contract is agreed, otherwise the contracting out provision would be of no effect. The effects of the terms must be clearly and unambiguously stated. The rejection of a claim by hull or cargo insurers due to failure of the assured shipowner to exercise due diligence in ensuring the vessel is seaworthy before and at the beginning of the voyage and breach of the warranty under the *MIA 1906*, means the shipowner's P&I club is expected to cover any loss which is a consequence of the unseaworthiness / cyberworthiness of the vessel but subject to the points discussed in paragraph 2.41. on this issue.

2.44. There is also no general exclusion of cyber risk in P&I cover but this is subject to agreement with its members.[174] Therefore, most P&I Clubs will cover the usual P&I liabilities arising from cyber-attacks / incidents but subject to Club rules where there are exclusions relating to losses, liabilities, costs and expenses incurred from the use of any electronic trading system other than those approved in writing by the club[175], 'unlawful, unsafe or unduly hazardous trade or voyage'[176], war risks and terrorism[177]. In spite of the non-existence of an explicit cyber exclusion

[174] Some P&I clubs have been more forthwith of their treatment of cyber risks in the additional covers to their P&I cover. UK War Risks Club Rules 2022 in Rule 4D.7.2 excludes the Association from any losses, liabilities, costs or expenses directly or indirectly caused by or contributed to by or arising from the use or operation as a means for inflicting harm, any computer virus. Britannia P&I additional insurance for policy year 2022/ 2023 (see n 176 below), Rule 4.1 excludes cover for 'loss directly or indirectly caused by, contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, software programme, malicious code, virus, computer process or any other electronic system'. The only exceptions are where the assured and the insurer agree in writing to waive this exclusion and in respect of risks of war loss which would otherwise be recoverable arising from the use of any computer system in the launch and or guidance system and or firing mechanism of any weapon or missile. If the computer system was not used or operated as a means for inflicting harm, the usual P&I liabilities would be recoverable, but this is subject to the other terms and conditions of the policy. Similarly, some P&I additional coverage include a War risks extension or The War Risks- Bio Chem Inclusion Clause, both of which excludes liabilities, costs, damage losses and expenses directly or indirectly from the use of any computer, software programme, electronic system used in the launch and or guidance and or firing mechanism of any weapon or missile. Notwithstanding, Standard Club, Bio-chemical risks inclusion clause 2022 (Clause 1.3) will cover the member where his liability was solely from the exclusion of liabilities and losses directly or indirectly caused by or contributed to by or arising from the use or operation of computer systems, programmes, virus, malicious codes as a means of inflicting harm.

[175] An example of this exclusion clause is Gard Rules 2022, Rule 63(j) < https://www.gard.no/web/publications/document/chapter?p_subdoc_id=1194646&p_document_id=781871> accessed 18 September 2022.

[176] Ibid Rule 74.

[177] Britannia P&I, 'Additional Insurances Policy Year 2022 /23: Part IV Clause 4.1' (Version 3.00 (February 2022) < https://britanniapandi.com/wp-content/uploads/2022/02/Additional-Insurances-2022.pdf> accessed 18 September 2022.

clause, shipowners must still take all reasonable measures to prevent or minimize the loss, liabilities and expense from a cyber-attack or incident. It is likely that the losses and liabilities proximately caused by the cyber and pirate attack would be covered by P&I clubs to the extent to which they are the type of liabilities usually insured and in other cases at the discretion of the managing committee through their omnibus rules. The recovery of an indemnity is only possible if none of the club exclusions become operative and cover is not affected by the shipowners' failure to maintain a certified cyber risk management system.

2.45. P&I clubs' omnibus rule is instrumental in protecting members against new risks which do not fall squarely within the ambit of the P&I coverage. The omnibus rule gives the managing committee the discretion to cover 'any liabilities, losses, costs and expenses incidental to the business of owning, operating or managing of a ship provided there shall be no recovery where the loss or damage is caused by a peril that is excluded from the Rules'.[178] The drawback is that the clause is totally dependent on the discretion of the managing committee and it is left to interpretation what is meant 'by incidental to the business of owning or operating or managing of a ship'. The question is not whether cyber risks will be regarded as incidental to owning, managing, or operating a vessel, rather the concern relates to the type and nature of the liabilities / losses and whether the costs and expenses were incurred to cover incidents / activities that are incidental to owning, managing or operating a vessel. Importantly, there shall be no recovery of loss or damage that is caused by a peril excluded in other provisions of the policy.

2.46. If that analysis is incorrect and the issue is whether cyber risks will be regarded as incidental to owning, managing or operating a vessel then a suitable response is yes, based on the nature of cyber risks. The reason for this is that vessels and their onshore management facilities rely on many information and operational technology tools which are inherently vulnerable to cyber-attacks. Furthermore, vessels and onshore facilities are lucrative targets for hackers and pirates because of the value of the vessel, the cargo onboard and data held by the vessel and offshore facility. Omnibus rules have been used to cover diverse set of liabilities for example, 'to

[178] The London P&I, 'Class 5 The Protecting and Indemnity Rules 2022/2023' 9.28.1 – 9.28.1.1 <https://www.londonpandi.com/documents/the-london-club-pplusi-rules-class-5-2022-2023/> accessed 18 September 2022.

cover the fees to repatriate pilots, crew refusal to work which is outside the control of the owner, expenses in releasing crew from prison and bill of damage after a night out while onshore' yet this is not reason to assume that a claim of the same type will be granted under the omnibus rules each time an application is made.[179] The diversity of claims means it is possible that the liabilities, losses or expenses arising from a cyber-attack will be of the nature to fall under the omnibus rule. The important feature is that the loss, damage is of the same genus as those covered by P&I clubs and they are not excluded from cover. Even so, each case will be decided on its own facts and based upon the discretion of the overseeing committee members and not dependent on a system of precedence.

D. Piracy under War Risks Insurance

2.47. Another option for the assured is to seek compensation from his war risk insurer. Like, the other Institute Clauses[180], cyber risks are not covered or excluded in the unamended form of Institute War and Strikes Clauses. The Institute War and Strikes Clauses Hulls -Time 95 in clause 5.1.6 excludes piracy from its cover but this shall not affect cover provided under Clause 1.4. Clause 1.4 covers loss of or damage to the vessel caused by strikers, locked out work men or person taking part in labour disturbances, riots or civil disturbances. Therefore, piracy will be covered under the Institute war and strikes clause only if the pirate attack is also riot or civil commotion. Loss caused by a person acting maliciously will be excluded if that person is a pirate as the exception in 5.1.6 does not apply to 1.5 (any terrorist or any person acting maliciously or from a political motive). Notwithstanding it is possible the shipowners will attempt to claim for the loss or damage to the vessel on grounds that the cyber piracy attack was caused by person acting maliciously in clause 1.5 of the Institute War and Strike Clauses Hulls. Where the Institute War and Strikes Clauses Hulls – Time (83) or (95) is incorporated in the assured's policies, the assured can purchase the Violent theft, Piracy and Barratry Extension [181] which amends the insured perils in clause 1 to include cover for violent theft by persons from outside the vessel, piracy and barratry

[179] Steven J Hazelwood and David Semark, *P.& I Clubs Law and Practice* (4th ed, Informa Law 2010) 10-280.
[180] Whereas piracy is listed as a peril in the Institute Hull Clauses, it is common practice to exclude piracy from marine hull cover through the incorporation of a violent theft, piracy and barratry exclusion (JH2005/046, 047 JH2005/048 (17 October 2005) which means some shipowners rely on their war risks policy to cover piracy.
[181] JW2005/002 (17 October 2005).

of masters, officers or crew. With the extension, the new Clause 4a states that a claim will not be paid for loss caused by violent theft by person from outside the vessel or piracy if the aggregate claim arising out of each accident or occurrence does not exceed the deductible agreed. This does not apply to claims for constructive total loss and its associated sue and labour claims arising from the same accident or occurrence.

2.48. The assured has the option to seek indemnification from a war risk provider such as Hellenic War Risk Club. For illustration purposes, reference is made to Hellenic War 2021 Rules which provide cover for losses, damage or expense to its Hull and Machinery as a result of piracy in clause 2A.2.6, protection and indemnity liabilities, costs and expenses relating to the crew caused by piracy in clause 2C.2.6 and there is no specific exclusion of cyber risks in the rules. That means if the owners of Orion were members of Hellenic War, they would be able to recover an indemnity for the losses incurred as a result of cyber and pirate attacks. Clause 2A.4.2.3 explains that even if the claims are recoverable under a standard hull insurance policy, the assured claim under their war risk policy will not be excluded.[182] Accordingly, there is no exclusion for double insurance therefore if both the hull and war risk insurers agree to pay, the expenses should be apportioned according to the liability of each insurer.[183] The amount recoverable will be subject to such deductible determined by the directors before the beginning of the policy year during which the claim arises.[184] If the amount claimed is the cash held onboard by the master or representative of the owner which was to be used for the vessel's business or trade, the maximum recoverable for each accident or occurrence of loss is US$20,000.[185] If the piracy results in actual or constructive total loss, the liability of the club in terms of the loss of the ship and the loss cash 'shall not exceed aggregate of the sum insured recoverable in accordance with Rule 2A.4 which sets the value on which the insurance is based and the sum if any insured in respect of freight and disbursements'.[186]

[182] Hellenic War Risks, 'Rules 2021 and ByeLaws: Risks Insured Clause 2A.4.2.3 and General Exclusions and Qualifications Clause 3.11.3' (HWR Rules 2021) <https://www.hellenicwarrisks.com/fileadmin/uploads/hellenic/Docs/PDFs/HWRB_Rulebook_2021_Policy_Year.pdf> accessed 18 September, 2022.
[183] MIA 1906, s. 80.
[184] Hellenic War Risks (n 182) Clause 3.15.2.
[185] ibid Clause 3.15.3.
[186] Hellenic War Risks (n 182) Clause 3.15.4.

The effect of the events of this scenario on the assured war risk insurance coverage will be the same as discussed above under the marine hull policy as there is no exclusion of cyber clause. Therefore, the war risk insurer will be expected to pay for the losses caused to Orion and his third party liabilities.

E. Is Kidnap and Ransom Insurance a viable option?

2.49. Traditional Kidnap and Ransom (K&R) insurance was designed to secure the release of crew members and other people onboard captured vessels, on condition that a request for ransom is paid to the pirates. K&R insurance protects the individual and company from the financial loss which may arise from the kidnap, extortion and ransom. Due to the increased incidence of cyberattacks specifically ransomwares, K&R insurers have been kept busy as assureds who are in a similar position to Orion's shipowner have been taking advantage of the extortion clause available in their K&R policies. These extortion clauses are being relied on by shipowners and other policyholders to cover cyber extortion / ransomware request. The positive response of some K&R insurers was consolation to assureds that provided they have not breached the contract of insurance, the ransom paid is likely to be reimbursed by their kidnap and ransom insurers. These kidnap and ransom policies usually have predetermined limits so if the owners of Orion had a K&R policy with a limit below £10 million, they would have to pay the balance on their own or seek the assistance of their P&I insurers who have made no commitment to meeting these costs but may exercise their discretion to fulfil the requests of their member.

2.50. Where the assured has a K&R insurance policy, it is expected that the K&R insurers will pay for the release of the crew and be secondary protection to the vessel while the hull or war insurers will pay for a proportion of the ransom for the release of the vessel.[187] The measures to determine how the liabilities should be divided among the insurers is not information which is readily available however if the ransom exceeds the limit under the K&R policy, the assured must ensure that the hull insurers will contribute higher than that limit. Since K&R policies were created

[187] Marsh, 'Piracy- the insurance implications' (2011) <http://static.igpandi.org/igpi_website/media/article_attachments/Marsh%20Piracy%20implications.pdf> accessed 18 September 2022.

specifically to address the facts in the scenario except for the cyber element, they offer a range of unique services which a hull or war risks insurer would not provide to the assured. These include consultation services, insurance for the ransom while in transit, interpreter fees, independent negotiator, medical and psychiatric assessment inter alia. While a typical K&R policy will cover many of the liabilities, they are not designed to address cyber risks thus their limits for pay out may be lower than what a cyber policy would provide for cyber extortion claim.[188] Typical cyber insurance include a limit of liability for cyber extortion ranging between GBP£1,000,000 to £ 3,000,000 whereas traditional K&R policies tend to advertise a limit of £100,000 to £1,000,000[189] for cyber extortion losses, an amount far below the potential loss from a ransomware or cyber extortion claims, also reflective here where the demand by the hackers is above the limit that most traditional K&R insurers would be willing to pay.

III. Exclusions and possible defences of the Insurer

2.51. Traditional hull and cargo policies currently offered in the marine sector will include a cyber clause, which excludes loss directly or indirectly from such risks. The most popular clause Institute Cyber Attack Exclusion Clause (CL.380) discussed extensively below, excludes 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 system, malicious code, computer virus or any other electronic system. To date, there has not been any judicial decision where the meaning of CL.380 has been interpreted. As such the terms of CL.380 will be given their literal and or purposive meaning as accepted within the legal and insurance sector. It is suggested that 'as a means of inflicting harm' should adopt the same meaning as 'malicious' which means that the hackers and pirates had to portray some element of 'spite or ill will or the like'[190] not necessarily directed at a specific person, goods or vessel. The intent of the hackers was to corrupt the ECDIS and GPS of the ship, an act which was inherently malicious, independent of the

[188] Suzanne Barlyn and Carolyn Cohn, 'Firms Turn to Kidnap Insurance Policies to Cover Ransomware Losses' (Insurance Journal, 19 May 2017)
< https://www.insurancejournal.com/news/international/2017/05/19/451637.htm> accessed 25 September 2022.
[189] These are figures noted on policy schedules that the researcher reviewed, and information received during conversations with brokers and insurers but given in confidence hence the reason the source is not stated.
[190] *Nishina Trading Co. Ltd v Chiyoda Fire & Marine Insurance Co. Ltd* [1969] 1 Lloyd's Rep 293, 298.

detainment of the vessel and crew by the pirates who were their accomplices. The entire mission was perpetrated by using a computer virus or malicious code to inflict harm and loss to the owners, charterers and all other stakeholders in the Orion and her voyage. The term to inflict harm should not be limited to physical damage but ought to include financial loss or to put the victims at risk of loss. On this premise, the combined act of the hackers and pirates will fall within the malicious act exception thus relinquishing the insurers from any obligation under the insurance contract.

2.52. When CL.380 is applied to the facts herein and if attached to a hull or cargo policy, the assured would be unable to recover from their hull or cargo insurers for their loss, expenses including the ransom paid to the cyber criminals and pirates. The attack was aimed at the vessel where the hackers intentionally penetrated the computer and navigation systems of the vessel by using a malicious code to inflict harm. The harm inflicted is in the form of the loss of data and control by the master and crew of the vessel and its redirection in the path of the pirates who captured Orion, held the crew captive and demanded the ransom which was paid to secure the release of the vessel and ensure the safety and protection of the crew and cargo. Whether the ransom, negotiation fees, bunker fees and the additional liability or expenses is the proximately caused by the cyber-attack is irrelevant since paragraph 1.1 of CL.380 displaces the default causative requirement in s.55 of the *MIA 1906*, extending the excluded loss to those indirectly caused by or arising from use or operation of the computer system or virus to inflict harm. Moreover, the exclusion is subject only to the war risk exception provided in clause 1.2. This means that even with the consensus that piracy is the proximate cause of the loss which should be recoverable under a hull policy and ICC A, with the incorporation of CL.380 piracy being the proximate cause of loss is irrelevant. The assureds' claims would fail because the expenses and liability were indirectly caused by the use or operation of the computer systems and the malicious code to inflict harm. In the same way, if the substitute causative arguments are accepted so that the loss was equally caused by the pirates and the cyber-attacks, the exclusion will prevail and likewise the insurers will not accept liability for the loss, damage and expenses from the attack.[191] If the current facts are placed under a traditional hull policy which incorporated CL.380, there will

[191] *P. Samuel v Dumas* (1924) 18 LIL Rep 211, 222.; *Wayne Tank and Pump Co Ltd v Employers Liability Insurance Corporation* [1974] QB 57, CA, 75.

be no payment or reimbursement for either sue and labour expenses or general average sacrifice because cyber risks were excluded from the policy. The shipowners of Orion would be in a predicament as they would now hope their P&I club will reimburse their liabilities and losses which are not guaranteed.[192]

2.53. CL.380 focuses on and applies only where there is an infliction of harm, which is a limitation of the policy if the computer system, virus or code was not used or operated to inflict harm on the assured shipowners. LMA5402 is the newer and more comprehensive 'Marine Cyber Exclusion' with its clause 1.1 excluding loss, damage, liability and expenses directly or indirectly caused by, contributed to by or arising from the failure, error or malfunction of any computer systems, code, virus, programmer, process or any other electronic system. Clause 1.2 is the exact form of clause 1.1 of CL.380 and excludes loss where computer system etc was used or operated to inflict harm. The incorporation or attachment of LMA5402 as a paramount clause to the shipowner's hull or cargo policy would result in the assured shipowner and cargo owners not being able to claim for the loss, liability, damage or expense from their hull and cargo insurers. LMA5402, unlike CL.380 also excludes cyber-attacks that were not intended to inflict harm on the assured. Even if the parties and the court decide that the proximate cause of the loss to the assured shipowners and cargo owners was the pirate attack, this is irrelevant because it operates to exclude all loss directly or indirectly caused by, contributed to by or arising from the use of the virus to inflict harm on the computer systems of Orion which contributed to the successful takeover by the pirates. The LMA5402 exclusion would completely absolve the insurers of all liability to the shipowners and cargo owners, who would be forced to seek compensation from their other insurers or worst-case scenario may need to pay these expenses directly from the company's account without any prospect of indemnification.

2.54. Standard hull and machinery and cargo policies include a war exclusion clause[193] which is paramount to any other clause in the policy. The question is whether the insurers war exclusion would be applicable to cyber-attack on the Orion or generally. War risks exclusions are quite clear,

[192] The P&I Club stance on ransom payments was discussed above at paragraphs 2.40.
[193] Clause 24 ITCH and clause 18 IVCH 1995; Clause 6 of ICC A 2009.

and assureds expect those exclusions when included in an all risks hull or cargo policy to become operative with regard to war in the traditional meaning of the word which involves the use of weapons, conflicts between states. It is not a term or clause which assureds would usually associate with a cyber-attack. If it was intended for the war exclusion to be applicable to cyber-attacks / cyber risks, the insurers should have amended the exclusion clause, so it is obvious to both the insurer and assured. This was the reasoning of the court in *Merck & Co. Inc and International Indemnity Ltd v Ace American Insurance Company, et al.*[194] where the Superior Court of New Jersey granted a summary judgement to Merck dismissing the insurers case that the war risk in the all risks property policy would operate to exclude any loss from the Notpetya cyber-attack which the insurers attributed to Russian government. In rejecting the insurer's case, the court emphasized that a war exclusion in an all risks policy has never before been applied to a cyber-attack. The insurer should have changed the words of the war or hostile act exclusion clause to reflect their intention not to cover cyber risk and since this was not done, the exclusion does not apply. The reasonable expectation of the assured is that the exclusion would apply to only traditional forms of warfare. Though this decision is not binding on courts in the UK, it is a strong reminder to parties that exclusions which are not specifically worded to exclude cyber risks may not be adequate to protect insurers against the risks of added liability from a cyber-attack which has caused an insured loss.

2.55. If there was no cyber exclusion clause, the hull insurers could attempt to reject this claim purely on the basis that they do not protect against damage to GPS and ECDIS which are navigational systems comprising of hardware, software and data[195], which to date have not been classified as machinery, damage to which claims can be made against hull and machinery insurers. Though unlikely, this will only change when the marine sector recognizes that 'physical loss' may need to include loss or damage to computer hardware, software, data and electronic damage. A similar reasoning may be applied to this issue as was discussed in *St Albans City and District*

[194] Docket No. UNN-L-2682-18 (Law Division, Union County).
<https://www.documentcloud.org/documents/21183337-merck-v-ace-american> accessed 18 September 2022.
[195] International Maritime Organisation, 'ECDIS Guidance' (MSC.1/Circ.1503/Rev.1 16 June 2017)

Council v International Computers Ltd[196] where Scott Baker J (obiter) made the point that previous cases have left open the issue of whether software is to be treated as goods under the *Sales of Goods Act 1979.* He however went on to state that 'software is probably goods within the Act.' Scott-Baker J made reference to the Australian case of *Toby Constructions Products Ltd v Computa Bar (Sales) Pty Ltd*[197] in which a distinction was made between the software on its own in the form of algorithms and where the software / program has been placed on a storage medium such as a disc, magnetic cards, magnetic tapes, discs, drums or magnetic bubbles' the more current equivalents would include Universal Serial Bus (USB)[198] and hard drives. The latter form is accepted as 'goods', physical damage to which is covered under most property and liability insurance.

2.56. The debate remains open particularly as it relates to insurance contracts and what is defined as physical damage in the maritime sector. However, if the reasoning from *St. Albans* is to be applied to marine insurance contracts, unless it is clearly defined in policies, it may be possible to define loss of data or software damage as physical damage. In fact, this approach has been encouraged by courts in the US where loss of computer data or disruption to computer system has been categorized as physical damage.[199] Conversely, there are also US cases which have rejected the notion of software being categorized as physical property such as the decision of *America Online, Inc v St. Paul Mercury Insurance Co*[200] where the court relied on the natural meaning of the word 'tangible' and held that since computer data, software and systems are incapable of being touched and are invisible to the human eye, they cannot be classified as tangible property for the purposes of the insurance contract between the parties. The court rejected as unpersuasive any reference to cases from outside the insurance context and specifically those for tax purposes[201] which held that computer data and software are tangible property. The attitude within the London

[196] [1995] F.S.R 686, 699; [1996] 4 All ER 481, 493 (CA). Though the decision in the High Court was partially reversed, Sir lain Glidewell (obiter) agreed that software on its own did not qualify as 'goods' but computer disks as tangible media could qualify as 'goods' within the definition of s. 18 Sale of Goods Act 1979 and s. 61 of the Supply of Goods and Services Act 1982.
[197] [1983] 2 NSW LR 48.
[198] Universal Serial Bus is device used for the storage and transfer of data between computer systems.
[199] *American Guarantee & Liability Insurance Cob Ingram Miero Inc* 2000 WL 726789 (A Ariz 2000).
[200] 207 F. Supp. 2d 459 (E.D. Va. 2002).
[201] Wal-Mart Stores, In., 696 So. 2d, 291.

marine sector seem to suggest the latter decisions will be the preferred route in line with the view that intangible losses should be covered by markets with the expertise in that area, that is cyber and product liability insurers. To escape this confusion, it may be best to clearly state that software damage will not be treated as physical damage for the purpose of the insurance contract. Otherwise, any ambiguity in the terms and what is being provided in the policy will be construed in favour of the insured against the insurers.

A. Piracy and the Malicious Acts Exclusion

2.57. Should the malicious intent of the cyber hackers prevent the ship owners from claiming their loss under these policies? The malicious acts exclusion mentioned earlier is provided under clause *26* and *23* of *ITCH* and *IVCH (95) respectively* and reads 'in no case shall this insurance cover loss damage or liability or expense arising from the detonation of an explosive, from any weapon of war and caused by a person acting maliciously or from a political motive' This clause is very specific, note as well that the conjunction 'and' is used by drafters to connect the subsections to the last part of the clause. This means that only if the pirates had either used an explosive or weapon of war while also acting maliciously or from a political motive could the insurers reject the claim on this ground. The malicious act exclusion is a paramount clause thus it overrides any endorsement or attachment to the insurance policy which is inconsistent with the terms of the exclusion. The meaning of the phrase '…person acting maliciously' was settled by the Supreme Court in the "B Atlantic" where it was explained that this refers to 'situations where persons act in ways which involves an element of spite or ill-will towards the property insured or other property or even a person resulting in loss of or damage to the insured vessel or cargo. It is not designed to cater for situations where the state of mind of spite, ill-will or the like is absent'.[202] Colman J in *'The Gracia Express'* stated that 'the words acting maliciously' should not be given a narrow interpretation and do not require proof that the person concerned had the purpose of

[202] *Navigators Insurance Company Limited and others (Respondents) v Atlasnavis-Navegacao LDA* (formerly *Bnavious-Navegacao LDA) (Appellant) [*2018] UKSC 26, paras 22 and 28. *The B Atlantic* applied Lord Denning, M.R. definition of 'malicious' in *Nishina Trading Co. Ltd. v. Chiyoda Fire and Marine Insurance Co. Ltd. (The Mandarin Star*) (C.A.) [1969] 1 Lloyd's Rep. 293, 298; [1969] 2 Q.B. 449.

injuring the assured or even knew the identity of the assured.'[203] Certainly on initial thought, it is reasonable to conclude that the hackers and the pirates were of the state of mind to spitefully cause loss or damage to the Orion and its shipowners when they introduced a malicious code on the vessel's computer system followed by the boarding of the vessel by the pirates who also attacked the crew, held them hostage and demanded a ransom. It would be just as malicious if the conduct was directed at the crew members, with the same consequential loss.

2.58. However, that conclusion may not be completely correct if we consider the decision in *The Salem*[204] in which it was decided that the deliberate destruction of the remaining cargo onboard the vessel 'was not a malicious act because it was the by-product of a larger operation carried out for gain'. Such conclusion was not disapproved when the case was heard by Court of Appeal.[205] Though Lord Mance in the *B Atlantic* expressed his hesitation about the narrowness of Mustil J treatment of the issue, he did not go as far as to declare it as wrong. That was the impetus for the same application in *McKeever v Northernreef Insurance Co SA* where Julia Dias QC sitting as Deputy High Court Judge decided that the smashing of the windows and padlocks of the yacht to facilitate looting of its contents was not a malicious act.[206] Likewise, if such reasoning is applied to the facts of this scenario, the cyber pirate attack was not a malicious act since spite or ill will of the hackers and pirates was absent. They did not intend to damage the vessel or hurt the crew. Their goal was to gain through the ransom that was paid to them. However, the technological aid together with the skills of the hackers may challenge and dispose of any contention that the attackers did not care about the identity of the vessel, crew and the cargo onboard. The hackers and pirates targeted Orion which is evidence to support the existence of malice or ill will towards the vessel even though some may disagree. Even, if those arguments are subject to doubt, what is absolute is that there is no 'malicious act' if the attack on the vessel was in furtherance of the unlawful instructions or fraudulent plans of the shipowners, though not the facts herein. In that

[203] *Strive Shipping Corporation& Another v Hellenic Mutual War Risks Association (The Grecia Express*) [2002] 2 Lloyd's Rep 88, 96.
[204] *Shell International Petroleum Co. Ltd v Caryl Antony Vaughan Gibbs (The "Salem")* 1981] 2 Lloyd's Rep. 316, 328 (Mustil J).
[205] [1982] 1 Lloyd's Rep 369.
[206] [2019] 2 Lloyd's Rep. 161 [89], [92].

sense, there would be either no or insufficient spite or ill will from the pirates who were permitted to enter the ship, not necessarily with the intent to harm the vessel or crew but to make a profit and assist the owners by carrying out their fraudulent plan.[207]

2.59. If the argument that the cyber pirate attack is not a malicious act is incorrect and the execution of 'a malicious act' was the only element necessary to trigger the operation of the malicious exclusion in clauses 26 and 23 of ITCH and IVCH 95 respectively, the insurers could rely on the exclusion to discharge them from any liability to the shipowners as a result of the cyber pirate attack. On the facts, there is no evidence of the use of weapons of war or explosives by the pirates. As such, an essential element of the 'malicious act' exclusion clause is absent, thus the malicious cyber pirate attack on its own without the use of a weapon or explosive would not trigger the operation of the exclusion. Therefore, even without a cyber exclusion clause, the malicious act exclusion would not take away cover for the cyber-piracy attack. If, however, there was evidence of the use of weapons of war or explosives by the pirates and or the cyber-attack be 'deemed a weapon of war', the exclusions in clause 26 and 23 of ITCH and IVCH 95 would deny the cover to the assured shipowners even if there was no cyber exclusion attached to the policy. As discussed above, If the policy incorporated the Institute War and Strikes Clauses as amended by the Violent Theft, Piracy and Barratry Extension and there is no cyber exclusion clause, the assured would be allowed to recover his loss from his insurers through clause 1.5 (any person acting maliciously) and 1.8 (piracy) provided the other conditions of the policy have been followed.

B. Unseaworthiness as a Defence: Insurers

2.60. It is an information technology flaw that caused the GPS and ECDIS systems of the Orion to be hacked through the use of an inexpensive GPS jammer. There is not much information in the facts about the type of information technology flaw that occurred yet the perceived ease at which the system was penetrated by hackers could possibly raise concerns about the seaworthiness[208] of

[207] *Suez Fortune Investments Ltd & Piraeus Bank AE v Talbot Underwriting Ltd & others ("The Brillante Virtuoso")* [2019] EWHC 2599 (Comm) [499].

[208] MIA 1906, section 39. The points discussed above in paras 2.41. – 2.43. on the issue of seaworthiness are also applicable here to the insurers reliance on 'seaworthiness' as a defence to the claim by shipowners or charterers. They will not be repeated except, briefly where necessary.

the vessel and if argued successfully will be a defence by the insurers to refuse paying for any loss due to this peril. A vessel is seaworthy if it is in a reasonable condition to encounter the ordinary perils of the sea that should be expected on the insured voyage.[209] This definition is complimented by Article III (1a) of the *Hague Visby Rules 1968 (HVR)* and the carriage of goods cases and that emphasize the need for the shipowner to exercise due diligence before and at the commencement of the intended voyage to make sure his vessel has the degree of fitness to withstand the ordinary perils of the sea and seaworthiness must be judged based on the reasonable standards and practices of the industry at the relevant time.[210] The provision under Article III (1a) of the HVR is nondelegable, therefore even if the carrier / shipowner has agreed with a third party contractor to manage, implement and monitor the cyber hygiene of the vessel but has not exercised due diligence in doing so, the carrier nor the shipowners would be able to rely on the defence in Art IV (ii) to relieve them from liability for loss or damage arising or resulting from unseaworthiness / uncyberworthiness of the vessel.

2.61. The burden is on the insurers to establish that the shipowners, captain and crew of Orion did not take reasonable measures to ensure that the Orion was cyber resilient. Since cyber risk is constantly evolving based on the pace at which technology develops, the owners could make the case that they have implemented the recommended best cybersecurity practices and have done all they reasonably could to ensure the crew and other employees were adequately trained to protect and respond to cyber-attacks. Despite best efforts, it is impossible to eliminate all cyber risks and the robustness of a vessel's cybersecurity is not defined by its ability to withstand all forms of electrical or digital attack where a computer system is manipulated to interrupt services or cause harm to the assured and other third party victims. Another basis for denying the claim is if the insurer proves the crew were negligent in their operation and manning of the vessel. The question may also be what exactly was the nautical position of the vessel when the attack occurred? If it was a situation where the crew did not correctly follow the mapping directions and were not actually in the sea zones allowed by their war policy, this suggest the crew would have deviated

[209] MIA 1906, section 39 (4).

[210] *McFadden v Blue Star Line* [1905] 1 KB 607; *Papera Traders Co. Ltd. and Others v. Hyundai Merchant Marine Co. Ltd. and Another (The Eurasian Dream)* [2002] EWHC 118 (Comm); [2002] 1 Lloyd's Rep. 719.

from their route before the cyber incident which is a significant breach of their insurance and carriage contract and would relieve the insurers of all liability to the shipowners / charterers.

IV. Cyber Insurance: Endorsement and Stand-alone Cyber Policies

A. Cyber Endorsement

2.62. The assured shipowner / cargo interests will be protected against cyber risk either through a cyber endorsement clause incorporated within their traditional marine insurance or through a cyber insurance policy. Marine Cyber Endorsement (LMA5403) is a limited write back of CL.380. In effect, LMA5403 operates as an endorsement clause in one sense and an exclusion clause in the other. Even though it is described generally as a cyber endorsement clause, LMA5403 excludes loss caused by the infliction of harm due to use of computers and electronic systems while endorsing cover for loss whether directly or indirectly caused by computer or electronic systems provided such use or operation was not a means for inflicting harm.

> **Marine Cyber Endorsement - LMA5403**[211]
>
> 1 Subject only to paragraph 3 below, in no case shall this insurance cover loss, damage, liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus, computer process or any other electronic system.
>
> 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.**
>
> 3 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, paragraph 1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

Paragraph 1 excludes loss, damage, liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation as means for inflicting harm of any computer

[211] LMA5403 (11 November 2019).

system, malicious code, virus, process or any other electronic system. Paragraph 1 is subject only to policies covering war risks, terrorism or any person acting from a political motive and where in normal circumstances, cover would have been provided for the loss arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile (paragraph 3). Through paragraph 2, the shipowners and charterers can recover any indemnity which would be otherwise recoverable under their marine policy to which the clause is attached. The claim shall not be affected by the use or operation of any computer system, programme, software, process or any electronic system provided such use or operation was not used as a means for inflicting harm.

2.63. LMA5403 has not clarified what is meant by the phrase 'as a means for inflicting harm' nor does it state to whom the harm should be directed or how 'harm' is to be interpreted. The malicious computer program affected the GPS and ECDIS of the vessel and rerouted it in the path of pirates who demanded and was paid £10 million in ransom. A limitation with this clause is that the cyber coverage offered when computer or electronic systems are not used as a means for inflicting harm is still subject to conditions, limitation, and exclusions of the policy to which the clause is attached thus covering only the usual perils but not those usually caused by a breach of computer system inter alia. The status of the clause in relation to the rest of the policy has also not been declared in that there is no express statement that it is a paramount clause, however this may be unnecessary since paragraph 2 supports the view that the clause is secondary to the rest of the policy. Consequently, even with this endorsement clause, the assured is not adequately protected against all types of cyber-risks, only those traditional marine losses which would normally be recoverable under the policy. Therefore, damage to the GPS and ECDIS, loss of data and other non-marine losses will not be recoverable, leaving the assured uninsured unless he is able to successfully claim under another policy. Moreover, the clause will cover loss directly or indirectly caused by a malicious code, programme or virus where it was intended to negatively affect the business of the assured, which in this scenario caused the assured shipowners to lose £10 million in ransom to save the vessel and crew. An expansive definition of harm should be adopted so that it includes both physical and non-tangible loss to the assured including software damage, data loss.

Such is immaterial because the clause and what is deemed recoverable is subject to the limitations and conditions of the traditional marine policy.

2.64. The assureds may be able to claim for their loss under their non-marine property insurance which usually excludes any loss arising directly or indirectly from a cyber incident / attack. To remove this gap in coverage, assureds may seek protection against cyber risks by attaching to their property insurance, a cyber and data endorsement clause such Property Cyber and Data Endorsement (LMA5400). The most relevant paragraphs of the clause are provided below:

> **Property Cyber and Data Endorsement – LMA5400**[212]
>
> 1 Notwithstanding any provision to the contrary within this Policy or any endorsement thereto this Policy excludes any:
>
> 1.1 Cyber Loss, unless subject to the provisions of paragraph 2;
>
> 1.2 ……
>
> 2 Subject to all the terms, conditions, limitations and exclusions of this Policy or any endorsement thereto, this Policy covers physical loss or physical damage to property insured under this Policy caused by any ensuing fire or explosion which directly results from a Cyber Incident, unless that Cyber Incident is caused by, contributed to by, resulting from, arising out of or in connection with a Cyber Act including, but not limited to, any action taken in controlling, preventing, suppressing or remediating any Cyber Act.
>
> 3 Subject to all the terms, conditions, limitations and exclusions of this Policy or any endorsement thereto, should Data Processing Media owned or operated by the Insured suffer physical loss or physical damage insured by this Policy, then this Policy will cover the cost to repair or replace the Data Processing Media itself plus the costs of copying the Data from back-up or from originals of a previous generation. These costs will not include research and engineering nor any costs of recreating, gathering or assembling the Data. If such media is not repaired, replaced or restored the basis of valuation shall be the cost of the blank Data Processing Media. However, this Policy excludes any amount pertaining to the value of such Data, to the Insured or any other party, even if such Data cannot be recreated, gathered or assembled
>
> 4 …..
>
> 5 This endorsement supersedes and, if in conflict with any other wording in the Policy or any endorsement thereto having a bearing on Cyber Loss, Data or Data Processing Media, replaces that wording.
>
> **Definitions**
>
> 6 Cyber Loss means any loss, damage, liability, claim, cost or expense of whatsoever nature directly or indirectly caused by, contributed to by, resulting from, arising out of or in connection with any Cyber Act or Cyber Incident including, but not limited to, any action taken in controlling, preventing, suppressing or remediating any Cyber Act or Cyber Incident.

[212] 11 November 2019.

7 Cyber Act means an unauthorised, malicious or criminal act or series of related unauthorised, malicious or criminal acts, regardless of time and place, or the threat or hoax thereof involving access to, processing of, use of or operation of any Computer System.

8 Cyber Incident means:

8.1 any error or omission or series of related errors or omissions involving access to, processing of, use of or operation of any Computer System; or

8.2 any partial or total unavailability or failure or series of related partial or total unavailability or failures to access, process, use or operate any Computer System.

9 Computer System means: …..

10 …

11 Data Processing Media means any property insured by this Policy on which Data can be stored but not the Data itself

Unlike LMA5403, paragraph 5 of LMA5400 assigns itself paramount status so it supersedes all other parts of the policy and if there is conflict in the wording which is related to cyber loss, the clause will replace that wording. Such pronouncement reduces the incidence of conflict between parties and any doubt that may persist in interpretation when the clause is attached to a policy. LMA5400 provides cyber protection in very limited circumstances where the cyber loss is the result of a fire or explosion that ensues from a cyber incident. The cyber protection afforded by the clause will still be subject to the terms, conditions and limitations and exclusion of the policy to which the clause is attached. However, there is no protection for such loss where the fire or explosion is caused by, contributed to by, resulting from, arising out of or in connection with a cyber act or any action taken in controlling, preventing, suppressing, or remediating any cyber act. LMA5400 excludes loss from a cyber act but covers loss from a cyber incident. The main difference between a cyber act and incident is that access was unauthorised and involved a malicious or criminal act whereas a cyber incident means any error or omissions involving access to, processing of, use of or operation of any computer system.

2.65. In comparison to LMA5403, in providing a definition and creating a distinction between cyber act and cyber incident, LMA5400 has partially resolved some of the uncertainties associated with LMA5403 use of the phrase ‘means of inflicting harm’ in deciding whether a malicious intent was required or alternatively whether a cyber loss caused by error or omission without evidence of a malicious element would suffice to trigger the operation of the policy and ultimately coverage

by the insurer. The actions of the hackers and pirates were unauthorised and criminal and should be categorised as cyber act from which indemnity for damage or loss is unrecoverable from the insurers. Further, the benefits of the endorsement would not apply to the scenario because the physical damage or loss, whether that be the damage or loss of cargo, the ransom was not caused by a fire or explosion. Additionally, the scope and effectiveness of the clause is restricted by its emphasis on physical damage with specific reference to covering the data processing media but not the data itself, similar to the arguments in the St Albans case. Damage or loss to the GPS and ECDIS software of the vessel is excluded from cover. While the traditional policies do cover physical damage, it is unlikely that damage to the GPS or loss of data or software will be considered 'physical damage' which is necessary for traditional policies to become operational.

2.66. The disadvantage associated with such policies is that they are often not written with the cyber needs of the company in mind thus they may not cover specific liabilities or the risks to which Orion's shipowners are most exposed. In other words, a typical marine insurance policy will not cover software or equipment damage, business interruption, reputational damage, data loss, cyber extortion or costs for loss of cargo due to a cyber incident. The attachment of a cyber endorsement clause to marine policies, will offer more protection against cyber risks when compared to marine policies that are silent on cyber risks. Yet, the limitations inherent in the language of endorsement clauses contribute to such policies not being the most comprehensive or adequate insurance response to cyber risks. As such some insurers have created cyber policies unique to the maritime sector, few of which will be examined to determine how adequate they are to address the facts of the scenario focusing primarily on assessing whether they provide more cyber protection to the assureds by examining what is covered under these cyber or cyber marine insurance policies?

B. Stand-alone Cyber insurance policies: Cyber marine policies

2.67. The practice so far has been to create bespoke cyber marine policies to address unique marine cyber risks, which can be distinct insurance policies or an extension of a traditional hull or

war cover. Beazley Insurers have developed a Cyber defence for Marine policy[213] which as the name suggests was created to address cyber risks to which the marine sector is most exposed. The policy in its original form focuses on protection against loss of hire and physical damage to vessels available as operational technology protection (OTP) and data and information technology protection (ITP). Under OTP the assured will be reimbursed for financial loss as a result of a cyber event which led to loss of hire and physical damage. This policy can be purchased either for a single commercial vessels and fleet with limits of US$ 5 million for loss of hire and US$50 million for physical damage. Each policy may be purchased as an extension of the marine hull policy which would cover typical hull and machinery liabilities to include sue and labour and general average costs. The physical damage limit is enough to cover the £10 million ransom paid by the assureds to the pirates which as discussed may be recovered as general average expense.

2.68. Even with the combination of the hull policy and the OTP, the professional services necessary to mitigate cyber or ransom situations are not provided under either policy. There is no provision made for consultation and public relations or crisis management services, insurance of ransom and ransom in transit or protection for the well-being of the crew. Without these services, the loss to the shipowners, charterers, crew and cargo interest may be greater as experts are not readily available to negotiate and quickly arrive at a settlement. An option would be for the assured to purchase the OTP and ITP policies where he would have access to the crisis management services complimented by the marine piracy policy also offered by Beazley. This combination of policies would offer the most comprehensive protection against the liabilities and expenses incurred due to the cyber and piracy attack on the Orion. EDGE Marine Cyber Insurance[214] is another insurance policy designed to address the cyber risk threatening the marine sector. Provision is made for losses arising from damage to the vessel because of a cyberattack, non-physical loss of hire, onshore business interruption, trade disruption, extortion and threat and liabilities and defence costs and a writeback for CL.380 exclusion. Norwegian Hull Club

[213] Beazley, 'Cyber Defence for Marine' (2019) <https://www.beazley.com/documents/Factsheets/beazley-cyber-marine-brochure.pdf> accessed 18 September 2022.

[214] EDGE, 'Marine Cyber Insurance' (2022) < http://edgegroup.com/portfolio/cyber-attack-exclusion-buyback-insurance/ > accessed 18 September 2022.

developed a Marine Cyber Threat and Extortion policy[215], the scope of which extends to the assured and its subsidiaries. Extortion payments are covered as well as the fees for crisis consultants to include negotiators, interpreters and public relations consultants and may include loss of hire and business interruption protection. There is also writeback for CL.380 clause. If either policy is purchased with a hull and machinery policy in place, the combined policies will protect the assureds against most of the liabilities and expenses incurred by the Orion, the extent of which will be subject to the limitations, conditions and exclusions of the policy.

2.69. Speaking of exclusions, some cyber marine policies for example SIGCo Cyber Hull Insurance clause 5.1.5 [216] excludes 'increased cost as a result of threat or hoax, in the absence of physical damage due to a cyber-attack'. The clause can be interpreted to exclude threats of ransomwares so that the insurers could deny the assureds claim for loss from the ransomware if they can prove it was not genuine or imminent attack but merely a 'threat' or hoax' and that the cyber-attack did not cause physical damage to the vessel. That will be a difficult task considering the forensic and visible evidence that the shipowners lost control of the navigation of the vessel when the GPS and ECDIS were compromised complimented by the digital and physical demand for ransom, the latter proved by the presence of the pirates onboard Orion and their refusal to disembark until there was confirmation from the hackers that the bitcoin transfer was received. Increased costs would include all costs related to the payment and transfer of the ransom including consultation fees and ransom paid, which suggests that usual costs would be recoverable notwithstanding that the attack of threat was hoax.

2.70. The insurers may attempt to argue that any physical damage to the vessel would have been proximately caused by the pirates and not due to the cyber-attack (if they are viewed as separate perils). However even if the damage to the vessel was caused by the pirates, the insurers would

[215] Norwegian Hull Club, 'Marine Cyber Threat and Extortion' (2022) <https://www.norclub.com/products-and-services/special-risks-marine-cyber-threat-and-exortion> accessed 15 March 2022. Please see working link below briefly describing the cyber threat and extortion policy that was offered by Norwegian Hull Club. It appears this policy has been removed or is being updated.
<https://www.norclub.com/insights/new-industry-guidelines-on-cyber-security-address-insurance-issues> accessed 25 September 2022.

[216] SIGCo Group, 'Cyber Hull Insurance' (v4- 21 July 2021)
< https://www.sigcogroup.com/docs/Policy_Wording_Revised_v1.4.pdf> accessed 18 September 2022.

still be liable for the loss because piracy is an excepted peril in the war risk exclusion clause 5.1.18 (b) found in the SIGCo. If piracy was an excluded peril, the cyber insurers would not be liable. The use of the malicious computer code to cause harm to Orion's navigation devices remains a cyber-attack even though the cyber criminals were in partnership with the pirates. The definition of cyber-attack in the SIGCO policy makes provision for such activities when it included the following words '… by any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organisation'. The general principles of marine insurance such as the sue and labour duties of the assured, general average and constructive total loss are also covered in the policy so that the points discussed above (para 2.29 - 2.39) relating to these principles are similarly applicable here. The maximum liability for any one occurrence[217] in the policy shall not exceed the total insured under the assured hull or total loss interest (marine or war risks) polices.[218] Mirroring the limits to that of the assured's hull policy makes commercial sense since the subject matter of the insurance is the vessel, and the insurer should not be expected to pay any amount beyond that value. If cover is provided under another policy for example the assured's hull or war risks policy, SIGCO insurers will only respond if the other insurances exclude or limit their liability in respect of the relevant loss or occurrence.

2.71. Another point on which the insurer will try to reject the claim is the successful application of clause 5.1.15 (d) 'failure or malfunction or inadequacy of any satellite' so that the insurers will not cover any liability or other losses arising out of or resulting, directly or indirectly from the malfunction of the GPS and ECDIS Orion. Their objection would be futile because the GPS and ECDIS did not fail, malfunction nor were they inadequate in the true sense of the words. There were no indications of internal faults with the devices which caused them to stop working nor was there evidence to support the claim that the assureds were negligent in maintaining or securing the devices, instead their function was impaired by the malicious code introduced to the system by the

[217] SIGCo (n 216) Clause 6.7. 'Occurrence means any one loss and or series of losses commencing during the Policy Period and arising out of and directly occasioned by one Cyber Attack'.
[218] Ibid Clause 3.1.

cyber criminals. There was a deliberate attack on the GPS and ECDIS, accordingly the exclusion in clause 5.1.15(d) does not operate to relieve the insurers of any liability to the assureds.

2.72. In addition to the specially designed cyber marine policies, the cyber insurance market has developed standalone cyber products, many of which include a cyber extortion or cyber ransom clause. If the shipowner is the holder of a cyber policy with such clause, there is the option to claim for the ransom and other related expenses from their cyber insurer, depending on the language and scope of the clause and subject to other conditions and exclusions of the policy. The adequacy of a cyber ransom clause in responding to the claims of the assured shipowner will be discussed in relation to sample cyber extortion clauses found in stand-alone cyber policies which are copied below:

> **Cyber ransom losses**[219]
>
> Following an illegal threat:
>
> 1. the reasonable and necessary fees of our appointed consultant, incurred by you with our prior written agreement, for advising you on the handling and negotiation of the ransom demand;
> 2. The cost of any ransom demand from the third-party or, if the demand is for goods or services, their market value at the time of the surrender, and
> 3. The amount of any stolen ransom, where such theft occurs at or in transit to the agreed location for payment of the ransom.

To be able to claim under this policy, Orion shipowners must meet certain conditions prior to the insurer making the payment for ransom. These conditions include the exercise of due diligence to ensure that before the ransom is paid or goods and services are surrendered, reasonable efforts are made to ensure that the threat was genuine and surrendered under duress.[220] The assured and no other individual outside that definition must have agreed to the ransom demands. Some policies

[219] Hiscox Cyber Clear Policy, 'Cyber and Data Insurance (WD-PIP-UK-CCLEAR (1) 19029 12/18)' Special Definitions Cyber ransom loss (2018) <https://www.hiscox.co.uk/sites/uk/files/documents/2019-03/19029-CyberClear-policy-wording.pdf> accessed 18 September 2022.
[220] ibid, Obligations Cyber extortion.

specifically state that it is a director who must have agreed to pay the ransom.[221] Likewise, the assured must either choose to inform law enforcements authorities (Action Fraud) about the threat or allow the insurers to do so. It is also expected that the assured would keep the insurers fully informed of all developments concerning ransom demands or any illegal threat.[222] One restriction is that some insurers will not cover more than one (1) claim arising from the same extortionist.[223] Additionally, the assured should take all steps to mitigate the loss and should not disclose the existence of cyber extortion cover except where such disclosure is required by law to the relevant law enforcement authorities. The reasoning behind nondisclosure of the existence of cyber endorsement cover is that cybercriminals and even insiders may be encouraged to target the assured as the likelihood of their request being met increases if there is insurance for such loss.

2.73. Whereas it is possible for the shipowners to recover the costs for the ransom under their cyber extortion policy, the limitations of a cyber data insurance policy as it relates to marine risks is that the shipowners would not be compensated by their cyber insurers if the negotiation fails, and the vessel is captured or lost. The same is true as it relates to the welfare of the crew. The cyber extortion payment is often linked to the risks of personal or sensitive business data being exposed or destroyed, denial of access to data if the ransom demand is not paid, so fees that a shipowner or charterer would incur for travel expenses for the family of the crew, medical and psychiatric care and other security expenses will not be covered by a cyber insurer. As such the assured would be left uninsured for extensive list of 'marine and seafarer' expenses and liabilities if they were to rely solely on their cyber extortion clause within their cyber policy. This would be inadequate protection for the shipowners / charterers but at the same time if cyber risks are excluded in all his other hull or property insurance policies, the assured will still be better off if he was able to recover the ransom paid, the consultation costs and guaranteed protection of the ransom monies while in transit from his cyber insurer. Although the cyber-attack on the Orion was followed by the pirates

[221] RSA Insurance plc, 'Cyber Risk Insurance Policy Wording: Cyber Risks Insuring Clauses 9 Cyber Extortion' (UKC05268A September 2018) <https://www.rsainsurance.co.uk/media/ruhfu0rp/cyber-risk-insurance-policy-wording-ukc05268a.pdf > accessed 18 September 2022.

[222] Hiscox (n 219).

[223] Aviva Insurance Ltd, 'Cyber Insurance Policy section : Extortion' (BCOAG15081 12.2020) <https://www.aviva.co.uk/adviser/documents/view/bcoag15081.pdf> accessed 18 September 2022.

capturing the vessel and holding the crew hostage, this would not prevent the assureds from being able to claim under their cyber policies if the threat and the ransom are related to denial of access to the computer systems or damage or loss to data.

2.74. Conversely, where the 'threat' to the assured is loss of the vessel or personal injury of the crew, the cyber insurers can object to the claim by insisting that they do not cover the risks to tangible property or personal injury to the crew of a vessel unless they are 'insured persons' as defined in the policy which often is restricted to a statutory director, partner or officer of the assured. In Hiscox Cyber Clear policy for example the cyber ransom loss clause presented above, refers to 'illegal threat' the definition of which is centred around 'damage or destruction of computer systems, data asset held electronically or the dissemination or use of electronically held commercial or personal information which may cause commercial harm if publicly exposed'. The 'illegal threat' can also be a cyber-attack which again is defined as a 'digital attack to disrupt access to or operation of a computer system'. The emphasis on digital access to or operation of computer systems and protection of data will be serious impediment to a successful claim by shipowners, charterers, and other stakeholders in the marine sector for cyber extortion loss where the threat or risk is not necessarily denial of access or risk of damage or exposure of personal and commercial data but where the threat and ransom paid are to protect the vessel, cargo, and crew. In scenarios where there is a threat of denial of access to the computer systems as well a threat to vessel and crew by pirates at sea, the most effective insurance response would be for cyber insurers to pay a proportion of the ransom in respect to the cyber extortion element of the risk and for marine hull or war risks and P&I insurers to cover the second element of the risks concerning the pirates, the risk to the vessel and crew. It is suggested that the proportion of liability is assessed based on the value of each insured asset and the limits related to each under their separate policies represented as a percentage of the total ransom paid. All other expenses to be covered by the respective insurer.

2.75. Having recognised the issues which may hinder a successful claim, the best option for the shipowners and charterers in Orion's position would be either to amend their kidnap and ransom policies so that they now include a cyber extortion clause; amend their hull so that there is a cyber piracy endorsement clause and or create a cyber marine piracy policy created specifically to protect

the shipowners and others from the risks of a cyber piracy attack which threatens to deny the release of the insured vessel, cargo and crew if the ransom is not paid. Ransom should be given an expansive meaning, so it is not limited to cash, marketable securities, goods or services but also cryptocurrency payments for cyber extortion.

C. Exclusions Under Cyber Policies

a. Bodily Injury or Property Damage

2.76. Most cyber liability insurers focus exclusively on nonphysical loss therefore it is often found that bodily and or property damage are excluded from pure cyber policies. The definition of physical injury includes emotional distress in some policies while it is excluded in others. The argument for emotional distress arising from a data breach to be accepted as a form of physical injury gained support following the decision in *Vidal-Hall and others v Google Inc*[224] where it was held that data subjects who have suffered material or non-material damage can a make claim for emotional distress without the need to prove they have suffered financial loss.[225] So, while cyber insurers will be prepared to cover the data breach costs or damage for each data subject within the limits of the policy, emotional distress or other forms of personal injury are not insurable under most policies. These claims would need to be pursued through other specialist insurance policy providers.

2.77. Destruction, loss or damage to tangible are often excluded from cyber insurance policies. Beazley in its Breach Response policy has clarified in its exclusion that electronic data will not be considered tangible property:

Bodily Injury or Property Damage

1. physical injury, sickness, disease or death of any person, including any mental anguish or emotional distress resulting from such physical injury, sickness, disease or death; or

[224] Vidal – Hall and others v Google Inc [2016] 2 All ER 337 [76] (Lord Dyson MR and Sharp LJ)*; Lloyd v Google LLC* [2018] EWHC 2599 (QB).
[225] See a more detailed discussion of the data breach issues in scenario 3 on the data breach onboard Santa Maria.

2. physical injury to or destruction of any tangible property, including the loss of use thereof; but electronic data will not be considered tangible property.[226]

This exclusion of damage or destruction to tangible property caused by or arising from a cyber-attack will absolve the cyber insurers from any liability for the equipment and cargo damaged or loss following the pirate attack on the vessel. This is a concerning insurance gap for assureds in the marine sector whose assets are prone to physical injury and damage particularly because most assets are transported in a physical state. This gap is created by the fact that tangible property damage and physical injury are excluded in cyber insurance policies at the same time cyber or computer related loss are excluded in H&M, cargo and most marine policies. Consequently, assureds must seek to purchase an additional cyber endorsement policy and or purchase cyber policies drafted specifically for those in the marine sector which will cover the unique risks of the sector. Despite these shortcomings, for parties within the marine sector, it is important that there is clarification in the 'Beazley Bodily Injury or Property Damage' clause that data will not be considered tangible property and so any loss incurred due to the destruction of data will not fall under the exclusion.

2.78. Cargo interests are not well protected against the risks of loss or damage if they seek an indemnity from a cyber liability insurer. Trading losses, loss of money and discounts exclusions found in some cyber insurance policies, for example Beazley Breach Response policy will not indemnify an assured for "any loss, transfer or theft of monies, securities or tangible property of the insured or others in the care, custody or control of the insured organization." Trading losses, loss of money and discount exclusion is wide enough to cover missed opportunities for cargo owners, charterers and owners while the vessel was being held at ransom by the pirates. Accordingly, the cyber insurer would not pay for lost contract, sale or delay in delivery of goods or services which results in discount in prices paid for cargo.

[226] Beazley, 'Beazley Breach Response policy: Exclusions Bodily Injury or Property Damage' (n.d) <https://policies.dppl.com/policy.php?policy_number=BBR-5A8ED7A3-8OEF> accessed 18 September 2022

V. Cyber Piracy under War Insurance Policy

2.79. Following the Lloyds Performance Management Supplemental Requirements & Guidance, published July 2020, all insurance and reinsurance policies written at Lloyd's must exclude all losses caused by war and nuclear, chemical, biological or radioactive risks (NCBR), except in limited circumstances.[227] This reinforces the exclusion of war and NCBR in hull and cargo and most cyber policies. Both cyber security data and privacy breach (CY) and cyber security property damage (CZ)[228] polices are among the exempted class of business which would be allowed to write war risks. However, when writing these cyber policies, the terms and scope of the cover must be clearly stated so silent cyber risks should not be an issue. If there is an extension of the policy to include war, that extension must not override any NCBR exclusions contained within the cyber policy. It is customary to follow local law or regulation on how coverage should be provided in policy documentation and for the exempted classes of business, it is recommended to follow local market practice. In light of these guidelines several war exclusions in varying degree of liability were developed to be endorsed on or attached to commercial cyber policies. It is not yet clear if the same clauses are or will become applicable to non cyber policies, but the discussion is relevant here should the cyber insurers attempt to deny the claim by stating that the cyber piracy attack on the Orion is a war risks thus any damage, loss or expense arising directly or directly from it will be excluded.

2.80. The exclusions (LMA5564, LMA5565, LMA5566, LMA5567)[229] are very similar in terms of the language used and excludes loss of any kind directly or indirectly occasioned by, happening through or in consequence of war or a cyber operation. The burden is on the insurer to prove that

---

[227] Lloyd's, 'Performance Management – Supplemental Requirements & Guidance' (July 2020) 41 <https://assets.lloyds.com/assets/performance-management-supplemental-requirements-and-guidance-july-2020highlighted/1/Performance%20Management%20Supplemental%20Requirements%20and%20Guidance%20July%202020Highlighted.pdf> accessed 18 September 2022. War and NCBR policies can only be provided where: the exclusion of war is prohibited by local legal or regulatory requirements, but this is not inclusive of the writing non-compulsory war risks; where the type of business is within the exempted class and where the syndicates have the express agreement from Lloyds through business planning process.

[228] Lloyd's, 'Cyber Risks & Exposures: Market Bulletin Ref: Y4842' (25 November 2014) <https://assets.lloyds.com/assets/y4842/1/Y4842.pdf > accessed 18 September 2022.

[229] LMA, 'Cyber War and Cyber Operation Exclusion Clauses' (LMA21-042-PD, 25 November 2021) <https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx> accessed 18 September 2022.

the exclusion applies. An obvious difference is the causal language used in each clause. 'Happening through' is not language commonly used in the marine sector, as such its meaning and what needs to be established to fulfil this causal effect requires clarification. Happening through should be treated as synonym for 'arising from'. Clauses 3-5 of each exclusion refer to the attribution of a cyber operation to a state and the definition of war and cyber operation are both related to the acts of a state against another state. War is defined as the 'use of physical force by a state against another state' thus excluding cyber incidents / attacks which may have the same effect but without physical use of force and not by a state against another state. Cyber operations mean the use of computer system by or on behalf of a state to disrupt, deny, degrade, manipulate or destroy information in a computer system of another state.[230] The emphasis on 'states' means that the exclusion would not be applicable to private acts of civilians who are not acting on behalf of their government or another state. Therefore, even if LMA5564 was attached to a cyber insurance policy of the assured shipowners, it would not operate to absolve the insurers of their liability since the acts of the pirates and hackers do not conform with the definition of war or cyber operations. Furthermore, it is doubtful whether cyber operation would extend to the damage or loss of cargo, vessel or even the ransom paid since the subject of a cyber operation is the 'information in a computer system'. Thus, if it is inapplicable to those type of loss and limited to acts against a state by another state, the exclusion will not be adequate to relieve the insurers from all liability from the cyber and pirate attack on the Orion.

2.81. In attributing cyber operation to a state, the primary but not exclusive determinant is whether the government of the state in which the computer system affected is physically located has attributed the cyber operations to another state or those acting on its behalf. Pending a decision, the insurer may rely on an inference which is objectively reasonable as to attribution of the cyber operation, but no loss shall be paid during this time. If the government of the state in which the affected computer system is located takes too long to decide or is unable to declare or does not

[230] Michael N Schmitt, 'The Use of Force' in Tallin *Manual 2.0 on the International Law Applicable to Cyber* Operations (2nd edition Cambridge University Press 2017) The Tallin Manual is a good but nonbinding legal source which explains how international law applies to cyber operations. It is in the process of a five (5) year review for the launch of Tallinn Manual 3.0.

determine attribution, the responsibility shifts to the insurer to determine attribution by using other evidence available to it. There are several problems with the terms of LMA5564, there is no explanation of the type and source of information the insurers should rely on to develop an inference and what will qualify as objectively reasonable and importantly who will sit as 'objective person'. The parties may disagree about what should be accepted as a reasonably objective inference. Furthermore, the reference to the insurer using 'such other evidence as is available' suggest that the insurer is permitted to rely on any source, type / quality of evidence available that will support his position that the exclusion does apply. In other words, the acceptable standard of evidence to support the insurer's 'inference' and to discharge his burden that the exclusion does apply is low and therefore prejudicial to the assured.

2.82. The second war, cyber war and cyber operation exclusion (LMA5565) differs from LMA5564 in that LMA5565 clause 1.1 to 1.3 list the conditions under which war and cyber operations are excluded. These are war or cyber operation carried out in the course of war and or retaliatory cyber operations between any specified state (China, France, Germany, Japan, UK or USA) and or a cyber operation that has a detrimental impact on the functioning of the state due to the direct or indirect effect of the cyber operation on the availability, integrity or delivery of an essential service in that state and or the security or defence of a state. Clause 3 introduces the agreed limits recoverable in relation to loss arising out of one cyber operation and a second limit for the aggregate for the period of insurance. If the limits are not specified, there will be no coverage for any loss arising from a cyber operation. Noteworthy is the fact that similar limits have not been introduced for loss arising from a war or cyber war, so the limit would be based on the insured value of the subject matter insured. The definition of essential service creates uncertainty because what may be categorised as 'essential for the maintenance of vital functions of a state' may vary across states. While examples are provided which includes financial, health or utility services, unless the parties stipulate and restrict this category to only the services named in the policy, there is potential contention between the parties over what will qualify as an essential service and what is a vital function to a state. It is expected that the marine sector will be among the list of essential services, however it is questionable and unlikely that a pirate attack on a

commercial private vessel would qualify as harm to an essential service, vital for function of the state.

2.83. A third form of the war, cyber war and cyber operations exclusion LMA5566 is identical to LMA5565 except that there is no equivalent to the clause on limits of liability for each cyber operation or aggregate loss in LMA5566. The fourth form of exclusion LMA5567 expounds on the listed condition mentioned in LMA5565 and LMA55666 particularly the exclusion or loss from retaliatory cyber operations between any of the specified states leading to two or more of those states becoming impacted states. The exclusion of cyber operation that has a major impact an essential service or the security of defence of a state shall not apply to the direct or indirect effect of a cyber operation on a bystanding cyber asset. LMA5567 introduces the concepts of impacted states and bystanding asset, thus expanding the effect of the exclusion clause. Impacted states means any state where the cyber operation has had a detrimental impact on the functioning of that state due to its effect on essential services and or the security or defence of that state. The bystanding cyber assets are computer systems used by the insured or its third-party provider that is not located in the impacted state but is affected by the cyber operation. As an exemption to the exclusion, the consequence is that the insurer will be exposed to liability for loss to assets that are not owned by the insured or its third-party providers. The only requirement being that these bystanding cyber assets / computer systems are used by the insured or its third-party providers which could be an extensive list of unidentified assets and liabilities. Another problem with the definition of bystanding cyber asset is it does not declare for what purpose the said asset should be used by the insured and the third-party provider; the presumption is the use should be related to the subject matter / business of the insured but without clarification, there are doubts about the scope and limits of the term. Interestingly and of concern is the use of the words ‘cyber war’ in the title of each exclusion but is not repeated in any of the four clauses nor is there a description of the meaning of a cyber war and how it differs from a cyber operation and war as defined in the clauses.

2.84. Guidance on the correct interpretation of the exclusion clauses was not published and given their deficiencies, the effectiveness of each exclusion clause is limited. In terms of their

application to marine activities and the facts of this scenario, the insurer will find that he is liable to indemnify the assured for his loss from cyber pirate attack unless there is evidence to attribute the acts of the pirates and cyber criminals to a state. Since the pirate attack is for personal gain, the language used in the exclusions would be more effective in scenarios where terrorist or political groups are involved. War is limited to acts between states and significant emphasis is placed on injury to essential services of a state, neither of which is exist in this scenario. To avoid liability for the cyber piracy attack, the cyber insurer would need to rely on other exclusion clauses in cyber insurance policy or the assured's failure to comply with cybersecurity warranties and conditions under the policy, the success of which is not absolute based in the issues in policy wordings raised throughout the discussion.

VI. Chapter Summary

Nature of the risks- cyber piracy

- Cyber piracy is a real risk to vessels and crew as the methods of attack by pirates are changing at the pace at which technology is being relied on in the shipping industry.

- Since vessels and marine onshore facilities are highly dependent on technology and are therefore prone to cyber risks, there is no reason why cyber risks cannot fall within section 3 of the MIA 1906 as a peril which is consequent on or incidental to the navigation of the seas.

Traditional Marine Insurance Policies

- Hull and machinery (H&M) insurers may reject any claim initiated by an assured arising from a cyber-attack, computer or electronic risks that results in nonphysical damage onboard the vessel. Damage to navigational instruments and systems for example the ECDIS are not the type of damage envisaged by hull insurers. In light of PRA SS4/17 and IMO MSC 428/98 it is good practice for insurers to state whether physical loss and damage include loss or damage to computer hardware, software, data and electronic damage.

- Without a cyber exclusion clause in the traditional insurance policies, claims would have been made requesting that H&M, War, K&R and cargo insurers cover loss or damage to IT and OT technology such as GPS and other computer hardware and systems due to a cyber-attack. Alternatively, if the cyber-attack is the proximate cause of the loss and there is a cyber exclusion clause, there will be no cover for any loss arising from the cyber pirate attack on Orion.

- The Institute Hull Time and Voyage Clauses do not list among perils covered or excluded damage or loss from a cyber, computer, electronic or technological element. Consequently, if there is no cyber exclusion clause, an assured who experiences loss or damage from a pirate attack that is equally attributable to the efforts of cyber criminals is likely to successfully claim against their hull insurers.

- H&M, War risk policies and P&I insurance may offer some protection against cyber risks, however such coverage will be inadequate as they will be limited to traditional marine perils which excludes cyber unique risks such as software and data loss, incident response and recovery costs, regulatory fines, intellectual property theft, business and contingent business interruption losses inter alia.

- The insurers could not rely on the malicious acts exclusions to deny the claim of the shipowners / charterers. The actions of cyber criminals and pirates will not qualify as 'malicious acts' under clause 23 and 26 of IVCH 95 and ITCH 95 respectively unless the loss, damage, liability or expense arise from the detonation of an explosive or from any weapon of war and caused by a person acting maliciously or from a political motive, which are not the facts in the scenario. However, the exclusion would apply, and the shipowners claim denied if the cyber criminals used their hacking skills to detonate an explosive or where they worked in tandem with pirates who used weapons of war to carry out the attack. These were not the facts of the scenario. The most viable option for the shipowner would be to rely on his war risks insurer to cover these losses since P&I clubs rules exclude war risks.

- Orion's shipowners could rely on the extortion clauses of K&R insurance policies provided they did not include a cyber exclusion. With the exception of physical losses, the K&R policy would cover losses such as ransom to release the crew only and operate as an additional layer of protection for the ship, consultation costs, insurance for the ransom while in transit, interpreter fees, independent negotiator, medical and psychiatric assessment, their pre-agreed limits for pay out may be lower than what a cyber policy would provide.

- P&I club rules do not exclude cyber and piracy therefore third-party liabilities that are usually insured by P&I clubs will remain covered when arising from a piracy incident, provided, as are the facts in this scenario, weapons of war and terrorism exclusions are not triggered. Generally, P&I clubs' position on ransom paid to pirates remain unchanged in that they will not indemnify the assured with monies paid for this purpose despite the cyber element or changes in the method of payment for example from cash to cryptocurrencies.

- Though unlikely, P&I clubs members committee may exercise their discretion under the omnibus rule by deciding to indemnify Orion's shipowners for the ransom paid to pirates or cyber criminals, however there is no legal obligation to do so.

- P&I clubs may reimburse shipowners for cargo contribution to which they would be entitled but which is irrecoverable due to the unseaworthiness of the vessel based on its poor cyber risk management, provided the breach does not also affect club cover.

- Some P&I clubs, particularly those that specialize in war risk (for example UK War Risks Club), exclude cover for losses, liabilities, costs or expenses directly or indirectly caused by or contributed to by or arising from the use or operation as means for inflicting harm of any computer virus. Therefore, if Orion's shipowner had such an exclusion in their P&I club rules the more unlikely that they will be indemnified for loss arising from the cyber piracy attack on the vessel.

Alternative Claims

- The ransom payment made by the shipowners to secure the release of a vessel can be either sue and labour expenses or general average contribution or sacrifice.

- Orion shipowners' claim to their insurers for a constructive total loss due to the cyber and pirate attack and the temporary loss of control of the vessel will fail since permanent deprival of access to the vessel is unlikely especially because efforts to negotiate a ransom is not behaviour to support a claim of abandonment on the basis that actual total loss was unavoidable as per s. 60 (1) of the MIA 1906. The situation reverses if the cyber-attack led to a collision which caused so much damage that it is not economically feasible to repair the vessel or alternatively if the pirates were more interested in keeping the vessel and cargo rather than a request for a ransom.

Cyber insurance Policies

- Many cyber insurance policies include an extortion clause which if widely construed may cover ransom expenses from a cyber piracy or other cyber related attacks, however any physical damage or loss of the vessel, cargo or crew would not be covered by the cyber insurer.

- Some policies, for example Beazley marine piracy insurance will indemnify the assured for the ransom paid, loss of ransom while in transit as well as effective crisis management to remedy the effects from the piracy. Ransoms have been paid in cryptocurrencies so a request of this nature would not on its own justify a denial of the claim by Orion's insurers.

- Orion shipowners most effective insurance options would be to acquire cyber protection either through a i) cyber endorsement clause for example LMA5403 (Marine Cyber Endorsement) and LMA400 (Property Cyber and Data Endorsement) incorporated within their traditional marine policy or ii) through a standalone cyber insurance policy (limitation / inadequacy mentioned in the first summary point). The endorsement clause is usually a write back of

CL.380 cyber exclusion but the disadvantage with endorsements is that many cyber specific liabilities such as pre and post crisis management services are omitted. So, even with a cyber endorsement, there will still be inadequacy of coverage as risk unique to cyber or the appropriate limits may not have been considered.

- To acquire the most comprehensive coverage; the assured may need to combine for example a hull policy with an ITP or purchase both an OTP and ITP policy. Even with the combination of a hull and the OTP policies, the shipowner' may still not be covered for liabilities such as ransoms, ransom in transit and the crisis management services. An option would be for the assured to have OTP and ITP as a comprehensive insurance package where he would receive the crisis management services and then purchase the marine piracy policy. This combination of policies would offer the most adequate protection against the liabilities and expenses incurred due to the cyber hack and a traditional pirate attack.

Way Forward

- The inadequacies of cyber endorsement clauses and traditional marine policies indicate the need for assureds to invest in a cyber insurance policy that reflects its cybersecurity vulnerabilities and ensure that gaps in other policies are covered in their cyber insurance.

- The requirement of force for an incident to qualify as piracy in maritime law may need to be amended to reflect the evolving digital landscape as there will be incidents where pirates take control of vessels with little or no 'threat or use of force' in the traditional sense of the word. Accordingly, the hacking and control of the GPS and ECDIS or any secured or critical network which leads to pirates detaining a vessel, cargo and crew against its will should satisfy the requirement of 'force'. In the absence of this basic component, where a cyber element is involved, assureds will find it difficult to claim under the piracy clause within their hull or war insurance.

- Insurers may deny a claim on the grounds of unseaworthiness / breach of the warranty of seaworthiness due to the lack of or inadequate cyber management and protection. The shipowners will counter any denial of claim if they demonstrate that they have implemented the best practices as recommended by industry and government regulators and that they have done all they reasonably could to ensure the crew and other employees were adequately trained to identify attack modes and respond immediately to a breach. The procedures used to assess the cyber resilience or ability of a business to withstand any form of computerized or digital attack cannot be static and resistant to change, otherwise the evolving nature of cyber risks would not be accounted for.

Scenario 2: Spear Phishing and Loss of Hire

Santos parent company network was hacked by cyber criminals; in fact, the attack was ongoing for several months before it was discovered. The investigations revealed that through a spear phishing attack, emails were sent to employees who upon opening the messages inadvertently gave the attackers access to the company data as their login was copied by the malware. The malware permitted the criminals to intercept communication between charterers and the company without their knowledge. Santos was on a time charter. Whenever transfer of hire were made, the criminals would intercept and take control of the communication to ensure the monies were directed to their accounts instead of the owners' accounts. The Hague Visby Rules 1968 were incorporated into the charterparty agreement.

Content **Pages**

I. Spear Phishing and Loss of Hire

A. The spear phishing attack through the eyes of management

3.1 Déjà vu! Is it a nightmare, is this really happening? Few years ago, Maersk was documented as one of the first shipping companies that publicly announced that they were targeted by cyber criminals. The reality of such events certainly played on our minds during board meetings, but we found comfort in the fact that we had ticked all the boxes and tried the utmost best to ensure that Santos company network was cyber secure and safe. The harsh truth is that the system was not safe and could not ward out the criminals who manipulated our computer systems through spear phishing attacks and sent misleading emails to all staff, fraudulently misrepresenting the source and authenticity of each email. The emails were from an address and written in a form that significantly replicates that of senior personnel hence garnered a high level of trust among the employees. Upon opening the emails, the employees were prompted to enter their company data, a technique used by the hackers to gain full access to more secure areas of the network. The hackers gained further success whenever requests were made to charterers for transfer of freight / hire, each request that was honoured was instead redirected to accounts set up by the hackers. So, while the charterers were of the impression that they had paid their dues, shipowners on the other hand were becoming frustrated having not received hire. The fraud continued for months before it was detected, by that time millions had been stolen.

3.2. The issue that needs to be decided is who should bear the loss of the stolen hire, technically the shipowners have not been paid so the charterers are in breach of the charter party arrangement. On the other hand, the charterers argue that they should not be made to pay twice and that as a result of the cyber-attack, the vessel has been offhire so they should instead be reimbursed by the owners as it was their negligence that caused their loss. Several questions will be answered, these include whether the vessel was off hire during the period of the cyber-attack, who should take responsibility for the hire that is lost and how will insurers respond? These issues will be addressed from both the perspective of the shipowner and the charterer. First, a brief summary of the nature of a charter party will be discussed then consideration will be given to several of the more widely used offhire clauses to represent a diverse cross- section of the marine sector. These clauses will

be analysed in tandem with current legal authority and practice direction. Secondly, we will discuss whether the responsibilities under the charter party agreement as it relates to hire should change when it has been established that a cyber element was involved. Thirdly, there will be an analysis of the insurance implications of the diversion of hire due to the spear phishing attack.

B. Fundamentals of a Charter-party agreement

3.3. The nature of a charterparty agreement and the rights and obligation of each party have been discussed extensively in leading textbooks[231] therefore there is little need for a detailed discourse on those topics. Instead, a brief summary of the current state of the law will be presented. In its most rudimentary form, a charterparty is the contractual arrangement between a shipowner and a charterer to use the ship for a period of time or for one or more voyages. This basic definition brings us to the two of the most widely used charterparty forms, the time charter and the voyage charter. The time charter as the name suggest is an agreement between the shipowner and the charterer for the latter to use the services of the vessel in exchange for hire which is to be paid in advance and full for the duration of the agreement. During the time charter, the shipowner will provide his vessel and his crew to the charterer who in turn has the right to exploit the vessel for his own economic benefits. Throughout the duration of the time charter, the master and crew will take orders from the charterer even though they are directly employed by the shipowner.[232] The charterer is only permitted to give employment orders and as such any decision relating to the navigation and management of the vessel is solely left to the master.[233] This means that if the charterer gives an 'illegitimate' order or any order which concerns navigation that may affect the safety of the vessel, cargo or crew the master has an obligation to refuse to follow such order.[234] If the master chooses to obey and any damage is incurred, the charterer will not be expected to indemnify the shipowner for the loss. In the alternative, if it is an employment order which resulted in the damage or loss, it is the obligation of the charterer to indemnify the shipowner.

[231] Terence Coghlin and others, *Time Charters* (7th edn, Informa 2014).
[232] The Aquacharm [1982] 1 Lloyd's Rep. 7.
[233] Whistler International v Kawasaki Kisen Kaisha Ltd (The Hill Harmony) [2001] 1 Lloyd's Rep. 147; Hyundai Merchant Marine Co Ltd v Furnace Withy (Australia) Pty (The Doric Pride) [2006] EWCA 559; [2006] 2 Lloyds Rep.
[234] The Gregos [1994] 1WLR 1465.

3.4. An important principle in time charters is the offhire clause where the charterers duty to pay hire ceases upon the occurrence of a named event often described in the contract. The offhire event usually prevents the full working of the vessel and is often but not always[235] the breach of an obligation which is the responsibility of the shipowner. There will be offhire events that are neither the breach of an obligation by either the shipowner or the charterer.[236] In addition to the navigation of the ship and care for the cargo[237,] the owner bears the expense of maintaining the ship and crew, carries the risk of marine accidents and must insure his interest in the vessel. In addition to the obligation to pay hire, the charterer must provide and pay for the fuel consumption and bears the risk associated with the trading of the vessel such as any damage to the hull during the loading of cargo and damage sustained based on an unsafe berth or port. This division of responsibilities, rights and obligations is fundamental to the lifeline of transactional relations of the time charter and the basis for determination of the allocation of risk between the parties.

3.5. On the other hand, the voyage charter is where the vessel is let to the charterer to be used for a specific voyage, for example from the Port of Swansea to Port Royal Jamaica. The remuneration for the use of the vessel is freight which unlike hire is not subject to the rules of set off.[238] Unlike the time charterer, the voyage charterer is not concerned too much with the length of time it takes to complete the voyage. It is instead, the shipowner who would be worried about saving time in order to make a profit. The concerns about time in the voyage charter is reflected in the principles of laytime and demurrage. Laytime is time agreed between the parties that loading and discharge should take. Once the time frame designated for laytime is exceeded, the charterer is obliged to pay the shipowner demurrage which equates to damages for the excess time. On a similar note, the shipowner owes the charterer the duty of proceeding with reasonable dispatch on the voyage. Failure to do so or any deviation from the voyage is a breach of the contractual terms of the charter which puts the charterer at risk of losing the benefits of his insurance protection.

[235] *The Ioanna [*1985] 2 Lloyd's Rep 164, 167 (Staughton J).
[236] *The 'Berge Sund'* [1993] 2 Lloyds Rep. 453, 460 (Staughton LJ).
[237] *The Doric Pride* [2006] 2 Lloyd's Rep. 175.
[238] *Aries Tanker Corp v Total Transport Ltd (The Aries)* [1977] 1 WLR 185, HL.

Even though a distinction has been made between the time and voyage charter, for the purposes of this discussion, the focus will be on the time charter.

C. Shipowners Claim

a. Time Charterers duty to pay hire

3.6. As mentioned above, the charterer is permitted to use and exploit the economic benefits of the vessel in exchange for the payment of hire to the shipowner and in the case of a sub-charter, to the charterer. This sum is to be paid continuously in full and in advance throughout the period of the charter party. This is an obligation which cannot be flouted or suspended for frivolous reasons particularly because the shipowner depends on the hire for the daily and overhead costs of financing the carriage. Lord Diplock explained this in ***The Scaptrade***:

> Hire is payable in advance in order to provide a fund from which the shipowner can meet those expenses of rendering the promised services to the charterer that he has undertaken to bear himself under the charterparty; in particular the wages and victualling of master and crew, the insurance of the vessel and her maintenance in such a state as will enable her to continue to comply with the warranty of performance.[239]

There are however occasions where the charterer is not forth coming with the hire as per the terms of the charterparty and this includes failure to adhere to the accepted form of payment. When it is agreed that hire should be paid in cash, the courts have not restricted cash to its literal meaning but have extended the meaning to include accepted bank transfers which would give the shipowner immediate control and disposable use of the money in the same way and degree that he would, had he been given the physical cash. The charterer has until midnight of the day on which the hire is due to be paid, therefore it is irrelevant that the bank has closed for the day. Any notice or withdrawal of the vessel before midnight on the due date is a breach by the shipowner.

[239] *Scandinavian Trading Tanker Co. A.B. Respondent and Flota Petrolera Ecuatoriana Appellants (The Scaptrade)* [1983] 2 A.C. 694, 702.

3.7. At common law, failure to pay hire in accordance with the terms of the contract is not to be treated as a condition therefore the shipowner cannot terminate the charter agreement based on late payment of hire. Commercial realities demanded a change in approach, specifically the potential economic hardship of the shipowner which meant that parties saw it fit and necessary to incorporate terms that would protect the interest of the shipowner by giving him the right to withdraw the vessel upon the charterers delay or failure to pay hire or to do so in the form agreed. The incorporation of such terms is to be found in many standard charter party forms for example lines 58 - 64 of the New York Produce Exchange (NYPE) form 1946:

> **Payment of said hire to be made** in New York **in cash in United States Currency**, semi - monthly **in advance**, and for the last half month or part of same the approximate amount of hire, and should same not cover the actual time, hire is to be paid for the balance day by day, as it becomes due, if so required by Owners, unless bank guarantee or deposit is made by the Charterers, otherwise failing the punctual and regular payment of the hire, or bank guarantee, **or on any breach of this Charter Party, the Owners shall be at liberty to withdraw the vessel from the service of the Charterers, without prejudice to any claim they (the Owners) may otherwise have on the Charterers**. Time to count from 7 a.m. on the working day following that on which written notice of readiness has been given to Charterers or their Agents before 4 p.m., but if required by Charterers, they to have the privilege of using vessel at once, such time used to count as hire.

It is immaterial what the reason is that led to the charterer's failure to comply with the terms of the hire, once breached despite the absence of malicious intentions or neglect, the shipowner has the right to withdraw from the charter party with immediate effect. This was not considered the most ideal situation for the charterers, accordingly newer versions of the NYPE form and other standard time charters provide the charterer with a grace period during which to correct the error. Noncompliance with the notice at the expiration of the grace period gives the shipowner the right to withdraw the vessel. The right to withdrawal of the vessel does not affect the shipowners right to claim damages or any other claim against the charterer. The shipowner may also suspend the performance of any other task under the charter agreement. Clause 11 of NYPE 93 is an example of the newer version of the hire clauses within standard time charterers with an anti-technicality provision:

> 11 a …Failing the punctual and regular payment of the hire, or on any fundamental breach whatsoever of this Charter Party, the Owners shall be at liberty to withdraw the Vessel from the service of the Charterers without prejudice to any claims they (the Owners) may otherwise

have on the Charterers. At any time after the expiry of the grace period provided in Sub-clause 11 (b) hereunder and while the hire is outstanding, the Owners shall, without prejudice to the liberty to withdraw, be entitled to withhold the performance of any and all of their obligations hereunder and shall have no responsibility whatsoever for any consequences thereof, in respect of which the Charterers hereby indemnify the Owners, and hire shall continue to accrue and any extra expenses resulting from such withholding shall be for the Charterers' account.

(b) *Grace Period*
Where there is failure to make punctual and regular payment of hire due to oversight, negligence, errors or omissions on the part of the Charterers or their bankers, the Charterers shall be given by the Owners clear banking days (as recognized at the agreed place of payment) written notice to rectify the failure, and when so rectified within those days following the Owners' notice, the payment shall stand as regular and punctual. Failure by the Charterers to pay the hire within days of their receiving the Owners' notice as provided herein, shall entitle the Owners to withdraw as set forth in Sub-clause 11 (a) above.

3.8. The privilege of the grace period in sub-clause (b) is dependent on the owners pinpointing that the non-payment of hire was caused by either of the qualifying events: oversight, negligence, errors or omissions on the part of the Charterers or their banks. Any error in judgment by the owners that results in the withdrawal of Santos without affording the charterers right to the grace period would be a breach of the contract on the part of the owners. On the current facts, since the failure to pay the hire was not due to either of the qualifying events in paragraph b, grace period observed or not, a withdrawal of the vessel by the owners would be a breach of the contract since the non-payment of hire was due to security breaches at the owners' company. NYPE 2015 provision has removed the qualifying events so that failure to make punctual payment of hire due for whatever reason will be a breach of their charterparty obligations.

The BIMCO Non-Payment of Hire Clause for Time Charter Parties 2006

(a) If the hire is not received by the Owners by midnight on the due date, the Owners may immediately following such non-payment suspend the performance of any or all of their obligations under this Charter Party (and, if they so suspend inform the Charterers accordingly) until such time as the payment is received by the Owners. Throughout any period of suspended performance under this Clause, the Vessel is to be and shall remain on hire. The Owners' right to suspend performance under this Clause shall be without prejudice to any other rights they may have under this Charterparty.

(b) The Owners shall notify the Charterers in writing within 24 running hours that the payment is overdue and must be received within 72 running hours from the time hire was due. If the payment is not received by the Owners within the number of running hours stated, the Owners may by giving written notice within 12 running hours withdraw the Vessel. The right to withdraw the Vessel shall not be dependent upon the Owners first exercising the right to

suspend performance of their obligations under this Charter Party pursuant to sub-clause (a). Further, such right of withdrawal shall be without prejudice to any other rights that the Owners may have under this Charter Party.

(c) The Charterers shall indemnify the Owners in respect of any liabilities incurred by the Owners under the Bill of Lading or any other contract of carriage as a consequence of the Owners' suspension of and/or withdrawal from any or all of their obligations under this Charter party.

(d) If, notwithstanding anything to the contrary in this Clause, the Owners choose not to exercise any of the rights afforded to them by this Clause in respect of any particular late payment of hire or a series of late payments of hire, this shall not be construed as a waiver of their right either to suspend performance under sub-clause (a) or to withdraw the Vessel under sub-clause (b) in respect of any subsequent late payment under this Charter Party.

The obligation to pay hire is absolute and the position is reinforced with the incorporation of BIMCO Non-payment of Hire Clauses 2006 in the charter party between the owners and the charterers. There is no condition or circumstance under which the charterer's failure to pay hire will be without repercussions. All that needs to exist is the non-receipt of the hire by midnight on the due date. The owners are not concerned that it was a cyber-attack which caused the delay in receiving the hire, what matters to the owners is that they retain the right to suspend the performance of any or all their obligations under the charter party. Additionally, the owners are free to exercise any other right they may have under the charter party. However, the shipowners cannot withdraw the vessel for arrears, only for the non-payment of hire when it first becomes due.[240]

3.9. Though drafted in the technological era, the BIMCO non-payment of hire clause is limited in its application in that there is no concession / provision made for cyber-attacks particularly where the charterer and shipowner exercised due diligence in making sure the hire is paid in advance and the vessel is seaworthy / cyber worthy respectively. To protect the charterers interest, the clause should be modified to address circumstances such as those in this scenario where the charterer transferred the hire, but it was not delivered to the shipowners account because the latter's

[240] *Quiana Navigation SA v Pacific Gulf Shipping (Singapore) Pte Ltd (Caravos Liberty)* [2019] EWHC 3171 (Comm).

computer/ payment system was compromised by a cyber-attack. Anti-technicality clauses are designed to account for technical failures outside the control of the charterers that was responsible for the delayed arrival of the hire in the owners' account. The anti-technicality clause gives the charter the opportunity to rectify the issue that prevented the delivery of the hire to the shipowner, but it is yet to be seen how these clauses will be treated where the shipowners or his agents were responsible or contributed to the non- payment of hire. The owners may decide to withdraw their vessel pursuant to paragraph (b) of the BIMCO Non-payment of Hire Clause 2006. Within 24 hours of the non-payment, the owners are required to notify the charterers in writing that the payment is overdue. If the payment is not received within 72 hours, the owners may by giving written notice within 12 hours withdraw the vessel. This right of withdrawal is not dependent on the owners first suspending performance neither does his decision to withdraw the vessel affect any other rights that the owner may have under the charter-party. However, the reasonableness of this approach may become a point of contention between the parties particularly where the charterers argue that this is an unfair demand since the cyber-attack which prevented the delivery of the payment was an attack on the shipowners' systems. As a result, the shipowner should not be allowed to withdraw his vessel and a charterer should not be made to repay hire if he followed the instructions and processes agreed for the transfer of hire. In fact, withdrawal of the vessel in these circumstances should perhaps be treated as a repudiatory breach of the contract by the shipowners. The fact that the charterers can prove that they took all steps to facilitate the punctual and full payment of hire, whether it be through bank receipts, or any agreed money transfer system should be adequate to avert any attempt by the owners to suspend performance or withdraw the vessel based on the non-receipt of hire. Furthermore, 72 hours may not be enough time to restore the system and test that it is safe to transfer another payment to the owners.

3.10. The obvious defence for the shipowners is that they complied with Article III (1) of the HVR in that before and at the beginning of the voyage the vessel was seaworthy. If this encompasses good cyber hygiene, their obligation would be discharged once the parties are satisfied before and at the beginning of the voyage that the shipowners exercised due diligence in ensuring that standard industry recommendations such as the IMO Guidelines on Maritime Cyber

Risk Management[241] and BIMCO Guidelines on cyber security onboard ships[242] and the International Safety Management Code have been implemented at their facilities ashore as well as onboard the vessel. Alternatively, and in the absence of the incorporation of the HVR in the charterparty, the carrier / shipowners' duty to ensure that the vessel maintains a good cyber hygiene should be given the same treatment as the common law treatment of the issue of seaworthiness. Thereby imposing on shipowners an ongoing duty throughout the voyage to have systems continually checked and monitored for any indication of security vulnerabilities and breach. The shipowners / carriers can also rely on Art IV (2)(a) of the HVR to discharge them from any liability arising from the cyber-attack which is due to the act, neglect or default of the master, mariner, pilot or the servants of the carrier in the navigation or management of the ship. Importantly, the management of the ship is distinguished from its navigation in that 'management' extends to systems and procedures implemented both ashore and onboard to facilitate the efficient and safe operation of the vessel.

3.11. The shipowner / carrier would not be able to rely on the exception in Article IV 2(a) if he is unable to prove that due diligence was exercised in ensuring that cyber security of the vessel is adequately protected which would be a breach of Art III (1) of the HRV. On the other hand, If due diligence was exercised in ensuring seaworthiness of the vessel but the loss was caused by the act, default or neglect of the servants of the carrier , the carrier may rely on the exception in Art IV 2 (a) to relieve him of any consequent liability.[243] To determine whether the negligent act was in the management of the vessel, there must be an 'examination of the nature and object of the acts which caused the loss and whether it was want of care of cargo or want of care of the vessel not

[241] IMO, 'Guidelines on Maritime Cyber Risk Management' (MSC-FAL.1/Cir.3, 5 July 2017) para 2.1.2 <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf> accessed 18 September 2022.

[242] Bimco and others, 'The Guidelines on Cyber Security Onboard Ships: Version 4' (Annex 4, 2020) <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)> accessed 23 March 2022. However, the extent to which the guidance is followed should be at the discretion of the master and shipowner.

[243] David Foxton and others, *Scrutton on Charterparties & Bills of Lading* (24th edn, Sweet & Maxwell 2019) para 11-115; *Gosse Millerd v Canadian Govt Merchant Marine* [1928] 1 K.B. 717, 749; [1929] A.C. 223 HL; *The Glenochil* [1896] P. 10, 15- 16, 19.

directly related to the cargo?'[244] The negligent act should be failure to take reasonable care of the vessel, if it is neglect to use an apparatus onboard the vessel to care for the cargo then that will not be 'management of the ship' to relieve the carrier of liability[245] Therefore, the focus is not the general business of transporting goods at sea.[246] In the *'Privocean'* the issue arose from the extra costs for strapping of the cargo which the charters contended was unnecessary and should be deducted from hire. Cockerill J held that 'the nature and object of the strapping was to stabilise the vessel which is related to ship management'.[247] The application of the principle to the scenario requires an answer to the question, whether the neglect to recognise and properly respond to the phishing email / a breach in the cyber security system measures onshore is want of care in the management of the vessel? Would the employee in the shipowners' office onshore be considered a servant of the carrier so that his neglect could qualify the application of the exception clause in Art IV 2(a) of the HVR? Management ashore[248] such as overloading in *Aquacharm*[249] and the costs of time lost because of extra strapping in *Privocean* have been approved as 'management of the ship', however since there is no standard definition of the term, its meaning will be formulated by the circumstances of each case and management of the shore may not necessarily amount to management of the ship even if the ship and cargo are affected.[250] However despite the threat to the safety of the vessel caused by the negligence of the employee who responded to the phishing email, this will not fall under the exception in Art IV 2 (a). It is accepted the instructions sent to the charterers by the employee was a function performed on behalf of the shipowners and in dealing with the ship. Providing payment instructions in response to an email purportedly from the charterers relates to the general business of transporting the cargo and not the management of the

[244] *Clearlake Shipping Pte Ltd v Privocean Shipping Ltd (The "Privocean*") [2018] EWHC 2460 (Comm); [2018] 2 Lloyd's Rep. 551 [61].
[245] *The Farrandoc* [1967] 2 Lloyd's Rep. 276.
[246] *Gosse Millerd v Canadian Govt Merchant Marine* [1929] A.C. 223, 233 HL (Lord Hailsham L.C citing Atkin LJ as he was then) in *Hourani v. Harrison* 32 Com. Cas. 305, 313, 319.
[247] *Clearlake Shipping Pte Ltd v Privocean Shipping Ltd (The "Privocean")* [2018] EWHC 2460 (Comm); [2018] 2 Lloyd's Rep. 551 [66], [76].
[248] *Suzuki & Co. Ltd v T. Beynon & Co. Ltd* [1926] 24 Lloyds's Rep 49, 54 (Lord Sumner) 'The term "management" may better fit the present case, but it is not a term of art; it has no precise legal meaning, and its application depends on the facts as appreciated by persons experienced in dealing with steamers. There is a management which is of the shore, and a management which is of the sea.'
[249] [1982] 1 Lloyd's Rep. 7.
[250] Richard Aikens and others, Bills of Lading (3rd ed, Informa 2020) 426.

ship and for that reason should not be allowed as an exception under Art IV 2(a) to relieve the shipowners of any liability to the charterers whether it be loss of hire or any other indemnification for losses incurred under the bill of lading.

3.12. Moreover, the management of the ship would now include cybersecurity risks prevention and incidence response mechanisms in accordance with *IMO Resolution MSC.428 (98)*[251] which indicated that Ship Management Systems (SMS) should consider cyber risk management based on the objectives of the ISM Code. As of 1 January 2021, administrators are obliged to ensure that cyber risks are appropriately addressed in SMS. ISM Code, section 4 requires that each company designates a person (s) ashore (DPA) who will maintain a direct link between the ship and the highest level of management ashore so as to ensure the safe operation of the vessel. The designated person is also responsible to ensure that there is adequate support and resources as required from ashore to the vessel. Parallel responsibility is placed on the company in section 3.3 to ensure adequate resources are provided to the designated person. The designated person may be the same as the company security office but if not, he will need to correspond with the company security and cyber security officers to coordinate the safe operation of the vessel which now includes cybersecurity plans. The document compliance holder is responsible for the management of cyber risks onboard the vessel and if the ship is under 3rd party management, the ship manager should reach an agreement with the shipowner.[252] Notwithstanding the practicality of the foregoing, it might not be possible to place the non-payment of hire responsibility on any of the persons in Article IV 2 (a) whether that be a master, mariner, pilot or servants of the carrier because these roles are limited to those working onboard the vessel and does not usually entail overseeing the

[251] IMO, 'Guidelines on Maritime Cyber Risks Management in Safety Risks Management Systems' (Resolution MSC.428 (98) adopted 16 June 2017) <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf> accessed 18 September 2022. Cyber risks management should include the following aspects: 'identifying and defining the role of users, key personnel and management both onboard the vessel and ashore; The identification of the systems, assets, data which if disrupted by cyber-attack could affect the operations and safety of the vessel; implementation of technical and procedural measures to protect against cyber-attacks, detect cyber incidents on a timely basis and ensure the continuity of operations; have a contingency plan which is regularly exercised' (part 1.1).

[252] Bimco and others, 'The Guidelines on Cyber Security Onboard Ships: Version 4' (Annex 4, 2020) part 1.6 <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)> accessed 23 March 2022.

security of the owners payment accounts or systems. However 'servants of the carrier' is wide enough to include the company security officer (CSO) whose task it is to ensure that the ship's security assessment is completed, the ship security plan is developed, approved, implemented and maintained and to liaison with port facility and ship security officers (PFSO and SSO).[253] The ship security officer will be onboard the vessel, is accountable to the master and responsible for the implementation and maintenance of the ship security plan. The cyber security officer (CySO) may also fall in the category of a servant of the carrier. His role is to coordinate the cybersecurity of the ship, report to the chief information security officer or the company's head of security depending on the size of the fleet, ensure periodic review and maintenance of the cybersecurity assessment and cybersecurity plan.[254] The CySO should also keep up to date with legal and regulatory changes and make the necessary adjustments to comply with those changes. Each officer in their specific roles contribute to the navigation or management of the vessel. Accordingly, there is the potential for Article IV 2 (a) of the HVR to extend to exclusion of liability for loss or damage as a result of security failure caused by the carrier's servants neglect or default in the management or navigation of the ship provided the carrier has exercised due diligence to maintain an adequate and properly implemented security management system at the company and onboard the vessel including the training of employees on cyber security risks. Here, however Article IV 2 (a) will not apply to absolve the shipowners of liability because as was already stated, the incorrect payment instruction is not an act done in the navigation or management of the ship.

3.13. If incorporated in the agreement, the owners are protected by BIMCO Non-payment of Hire Clauses 2006 (c) which provides them with an indemnity from the charterers for liabilities that may arise under a bill of lading as a result of the suspension and or withdrawal of the vessel. In referring to the bill of lading, consideration must be given to the cargo interest and any damage to the cargo due to the delay from the ship being off hire. If the owners cannot suspend their services or withdraw the vessel due to the cyber-attack being their fault, the charterers would not be obliged to indemnify the owners for liabilities that may arise under the bill of lading. In relation

[253] Hugh Boyes and Roy Isbell, 'Code of Practice: Cyber Security for Ships' (IET 2017) 7 <https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-for-ships/> accessed 18 September 2022.
[254] ibid 27 -28.

to the current facts the question is, will the shipowners be able to rely on sub-clause 'c' to recover an indemnity from the charterers for a breach that was outside the charterers control and was due to the fault of the shipowners? The cyber risks element involved here does not affect the law relating to shipowners right to an indemnity. The indemnity principle was not created to benefit the recipient for his wrongdoing, negligence or omission.[255] In fact, the rule is that the shipowner will not be indemnified for loss, damage or liability to which he has expressly or impliedly agreed; the loss, damage or liability must be caused by the charterers' lawful order as to the employment of the ship.[256] The loss must be of such nature that on the fair reading of the charterparty, the shipowner could not have accepted that risks.[257] The charterers employment orders was not responsible for the loss of hire. The shipowners intervening negligence would disentitle them from relying on subclause c to successfully claim an indemnity from the charterers.[258]

3.14. The court in '*White Rose*'[259] explained this principle where in that case a stevedore appointed by the charterers suffered injuries when he left his workstation on his own volition and for his personal need fell into an unfenced hatch. The stevedore sued the shipowners for his injuries who in turn claimed, an indemnity from the charterers. The shipowners' claim was rejected as the injury to the stevedore was caused by the contributory negligence of the stevedore and the shipowner who did not provide a safe working environment by ensuring that the hatch is fenced. The injury to the stevedore was not in any way the fault of the charterers. In the same way, a claim for indemnity by a shipowner who has wrongfully withdrawn his vessel for non-payment of hire which was not due to the default or omission of the charterer but was rather due to a spear phishing attack on the shipowners' system and involving his employees should not be permitted. Furthermore, while a shipowner will usually be indemnified for losses incurred as a result of following the charterers employment orders, the same is not true for navigation, seaworthiness or general safety of the vessel.[260] Therefore, even though subclause c is an express indemnity clause,

[255] *The "Nogar Marin"* [1988] 1 Lloyd's Rep 412, 422.
[256] *The Island Archon* [1994] 2 Ll. Rep. 227, 234 -236 (Evans LJ).
[257] ibid 238 (Nicholls V-C).
[258] *"White Rose"* [1969] 2 Ll. Rep. 52, 59.
[259] Ibid.
[260] *The "Hill Harmony"* [2001] 1 Lloyd's Rep 147, 153.

it is unlikely to extend to losses or liabilities incurred as a result of a cyber-attack which is partially due to the negligence or omission of the shipowner and especially because the cyber-attack affects the general safety of the vessel which is responsibility that remains with the shipowner in a time charter. There is the likely argument that the shipowners in agreeing to the method of payment and communication, through online bank transfer and without further verification 'agreed to run' the risk of exactly what happened with Santos, thus they should not be able to recover an indemnity from the charterers for liabilities incurred as a result.[261] To be protected against such risk, the parties will need to agree on a clause which clearly states how liabilities from a cyber-attack will be apportioned between the parties for example the BIMCO ISPS/MTSA Clause for Time Charters 2005[262] incorporated in NYPE 2015 or BIMCO Cyber security Clause.

3.15. If the parties had incorporated NYPE 2015, the debate as to the apportionment or acceptance of liability for cybersecurity breaches would have been long settled. NYPE 2015, clauses 44 and 45 follows the charterparty precedent and places responsibility on the owners to make sure the ship and company comply with the ISM and the ISPS Code during the charter period. Owners are liable for loss, damages, expenses, or delay that may result from noncompliance with the ISPS code and relevant amendments.[263] There is a requirement for the exchange of contact details between the charterers and the shipowners; clause 45 (a) (ii) provides that upon the request of the charterers the owners shall provide the full contact details of the company security officer along with a copy of the relevant interim or international ship security certificate. Likewise, clause 45 (b) (i) makes it mandatory for the charterers to provide their full contact details and if permitted under the charter party, the full details of the sub charterers. Except as otherwise provided in the charter party, any delay or expense inter alia which results from the non-provision of such details

[261] *Island Archon"* (1994) 2 Ll. Rep. 236.

[262] An example of such a clause is paragraph (a) (iii) which provides that: 'Loss, damages, expense or delay (excluding consequential loss, damages, expense or delay) caused by failure on the part of the Owners or "the Company"/ "Owner" to comply with the requirements of the ISPS Code/MTSA or this Clause shall be for the Owners' account, except as otherwise provided in this Charter Party.'
BIMCO, 'ISPS /MTSA for Time Charter Parties 2005' (Originally published in BIMCO Special Circular No. 5, 15 June 2005 - BIMCO ISPS Clauses Revised) < https://www.bimco.org/contracts-and-clauses/bimco-clauses/current/isps-mtsa_clause_for_time_charter_parties_2005> accessed 18 September 2022.'

[263] BIMCO, ASBA and SMF, 'NYPE 2015: Clause 45 (a) (iii)' (2015)
<https://www.bimco.org/Contracts-and-clauses/BIMCO-Contracts/~/link.aspx?_id=EEBE70C0DDB44328BFE184C79D2BA623&_z=z#> accessed 18 September 2022.

will be for the charterers account.[264] All security plans related to the ship are for the owners' account. All port related security matters are the responsibility of the charterer except where such costs or expenses are result of the negligence of the master, owners or crew, or the previous port visited, nationality of crew or ship which would be on the owners account.[265] So, even without the inclusion of an offhire clause, if the charterparty between Santos and the charterers was written on NYPE 2015, the outcome would be the same as at common law where the shipowners are liable for expenses related to the management and security of the vessel and company.

b. Financial Institution Liability

3.16. On the matter of liability and indemnity, what if the cyber-attack was directed at the shipowners' bank after cyber criminals identified vulnerabilities in their payment and money transfer products? Would the bank be held liable so that the shipowners can request an indemnity from the bank? Quite an unusual situation but the answer all depends on the relationship that exists between the bank and the shipowners. To the knowledge of the author, this issue has not been addressed in the UK[266], but there is an appetite for this in the USA subsequent to decisions from a First Circuit Court of Appeal in Boston and a Federal District court in Detroit where both courts found the bank liable for funds stolen by hackers from the accounts of small businesses. Both cases along with decisions from the UK Financial Ombudsman will be discussed to illustrate the legal position.

[264] Ibid.

[265] ibid Clause 45 (c)

[266] The Senior Management Regime (as set out in the Financial Services and Markets Act 2000) to which the banking sector subscribes permits the personal imposition of liability on senior management with a duty of responsibility for an area if he does not take reasonable steps to prevent or stop regulatory breaches from occurring and continuing to occur. The aim of the SMR is to encourage better services for customers by changing the behavioural culture in the sector through greater levels of personal accountability. Therefore, a senior manager who was negligent or omitted to take reasonable measures to ensure the payment systems of the bank was cyber secure or at the least had adequate and multiple step verification processes before a new or unusual transfer is completed may be held accountable for the breach. However, shipowners and charterers alike would prefer to be in court with a bank rather than an individual who may not have the means to compensate him for the losses incurred. So, a prudent legal team would encourage charterers and shipowners, to include the bank in whatever claim is being made for compensation. Further development or analysis of this point is beyond the scope of this research.

3.17. *Patco Construction Co. v People's United Bank*[267], the Claimant Patco had business accounts at a subsidiary of the Defendant. In 2009 Patco reported that over $580 000 was stolen through online transactions from its account by unknown third parties who accessed the account by providing the correct personal and security details of an employee of Patco. The money was sent to several individuals. Several security features should have alerted the bank to the breach, including the unusually high risk scores ranging from 563 to 790, high above Patco's usual risk score ranged from 10 to 214 and above the general 750 score which is considered high risks. Despite this high-risk score, the bank did not investigate and Patco was not contacted for verification purposes. Between May 8th and 13th, there were four (4) other transactions directed to individuals and paid at a time and in value inconsistent with Patco's regular payments.[268] It was not until the 14th May when Patco informed the bank that they did not authorize the transactions that they were flagged as fraudulent transactions. The total deducted from the account was $588 851.26 of which $243, 406.83 was recovered. Rather than taking any form of responsibility, the bank simply advised Patco about preventative and mitigating factors to protect their computer systems from security breaches. Patco's claim allege that the bank should bear the loss because i) its security system was not commercially reasonable in accordance with *Article 4A of the Uniform Commercial Code (UCC)*, codified under Maine Law at *Me.Rev.Stat.Ann. tit. 11, § 4-1101 et seq*[269], ii) the bank was negligent, iii) breach of contract, iv) breach of fiduciary duty, v) unjust enrichment and vi) conversion.

3.18. Prior to these fraudulent transactions, the bank implemented a new multifactor authentication system in accordance with the guidelines issued by the *Federal Financial Institutions Examination Council (FFIEC)* in 2005. The District Court held in favour of the Defendant finding though the security system was not the best, it was commercially reasonable since the bank implemented the multifactor authentication as recommended by the FFIEC 2005

[267] 684 F.3d 197, 199 (1st Cir. 2012).
[268] 684 F.3d 197, 199 (1st Cir. 2012) para D: "The transactions were entirely uncharacteristic of Patco's ordinary transactions: that were directed to accounts to which Patco had never before transferred money: they originated from computers Patco has never before used: they originated from an IP address that Patco had never before used; and they specified payment amounts significantly higher that the payments Patco ordinarily made to third parties."
[269] Governs the rights, duties and liabilities of banks and their commercial customers with respect to electronic funds transfers.

guidelines. The First Circuit court reversed the decision of the District Court by categorically stating that 'the bank's collective failures, taken as a whole, rendered the bank's security procedures 'commercially unreasonable' on several grounds including the bank's undermining of the security system by requiring multifactor authentications for all transactions above $1 which means that it was more difficult for the system to identify suspicious transaction. Also, the bank's poor monitoring of high -risk transactions was labelled unreasonable practices which collectively influenced the Circuit Court to determine that the Bank's security procedures were commercially unreasonable. The Circuit court decision was criticized for diverting from the precedent on bank liability to customers where in prior cases banks were discharged of any liability to the customer provided the bank instituted commercially reasonable security measures, a threshold met once the FFIEC guidelines were followed.[270] Notwithstanding the bank's adherence to these guidelines, the court did not agree those measures were adequate to discharge the bank of all liability to Patco. The case therefore raised the threshold of what is expected of banks yet the details of the obligations of a commercial customer under *Article 4A of the UCC* or where the bank's security system is deemed commercially unreasonable were not discussed.

3.19. Financial institutions are rarely held liable to their customers but there is no principle which generally prevents such liability except where there is an exemption clause under the contract. The extent of the bank's liability will depend on if the cause of action is founded in tort, contract or under the Data Protection Act 2018.[271] The Financial Conduct Authority states that with online financial transfer fraud, the general practice is to first determine whether the transaction has been authorized by the customer, which is the same approach taken by the courts in some the USA case discussed above. If the financial organization can prove that the transaction has been authorized by the customer, the starting point is that the bank will not be liable to reimburse the customer funds lost in transit. It therefore means the bank will be liable for 'unauthorised transfers'. The determination of which transfer is authorized versus those that are not authorized is fact dependent

[270] Robert K. Burrow, *Increased Bank Liability for Online Fraud: The Effect of Patco Construction Co. v. People's United Bank*, 17 N.C. Banking Inst. 381 (2013) pages 382 and 392 <https://scholarship.law.unc.edu/ncbi/vol17/iss1/16/> accessed 18 September 2022.

[271] We will not focus on breaches under the DPA / GDPR 2018 since there has been an extensive discussion of the principles under the DPA 2018 in the scenario 3 on data breach.

but arbitrary in the sense that simply because the sign in details and security questions have been answered correctly does not necessarily mean that the transaction was authorized by the account holder. In this scenario, the charterers transferred the hire to the new account on the advice of the employees of the ship owners so on that fact, the bank will argue that the transaction was authorized and thus the parties must bear their loss independent of the bank. The bank will not indemnify the shipowners neither will they reimburse the charterer. They will also attempt to reason that the shipowners and charterers failed to ensure their accounts were secure.

3.20. One case study from the financial Ombudsman focused on Nadia who was scammed through social engineering and made to believe that she needed to transfer all her money to another bank account in a foreign country to protect her from internal fraud at her current bank. Nadia went to the bank and personally made all the withdrawals and authorized all transfer to the new account. The bank asked Nadia questions about the transactions to which she provided the 'correct answers' however according to the financial ombudsman, 'based on her previous account activity, the bank had enough information to know that her behaviour and the nature of the transaction was out of character so the bank should have asked more questions and follow the guidance set out in the banking protocol. The bank was told by the Financial Ombudsman to 'reimburse Nadia the £100 000 and the interest she lost because the money was not in her savings account and a payment for trouble and upset, she suffered as a result of the bank's actions'.[272]

c. Social Engineering and Computer Fraud Policies: 'Direct Loss Test' and 'Unauthorised Access Exclusion'

3.21. Other cases in the USA looking at funds transfer through fraudulent means particularly phishing and social engineering focus on the 'direct loss requirement' and the 'unauthorized access exclusion'.[273] In *Pestmaster Services Inc v Travelers Casualty and Surety Company of America*[274]

[272] Financial Ombudsman Services 'Customer was asked to transfer money as her account was under threat' (n.d) < https://www.financial-ombudsman.org.uk/decisions-case-studies/case-studies/customer-asked-transfer-money-account-threat > accessed 18 September 2022.

[273] Celso de Azevedo, *Cyber Risks Insurance* (1st edn, Sweet & Maxwell 2019) 170-182. A full discussion of these cases and arguments are presented in the pages referenced.

[274] No. CV 13-5039-JFW, 2014 Westlaw 3844627, page 8 (C.D. Ca. July 8, 2014); 2016 WL 4056068 (9th Cir. July 29, 2016).

the payroll service provider of the assured Pestmaster Services Inc, stole money from the assured's account. The payroll provider had permission to transfer funds from the assured's account some of which were to be remitted to Internal Revenue Service (IRS) but this was done and was used instead for its own purposes. The crime policy which the assured relied upon included a funds transfer clause which protected the assured against the 'direct loss of money' held in bank accounts. The policy also provided that the computer fraud coverage indemnified the assured for loss of money directly caused by the computer fraud. The court did not agree that the transfer by the payroll provider was covered under the Funds Transfer clause as that clause did not cover transactions that were authorized by the assured even if the transfer were to further a fraudulent scheme. There was no evidence that the payroll service provider illegally entered the Paymaster's bank transfer system nor was fraudulent instructions given to the bank to complete the transfer. This did not satisfy the 'hacking' activities that the policy was created to cover. Additionally, the fraudulent conduct occurred only after the authorised transfer and the payroll service provider's use of its computer was incidental to and not directly related to Pestmaster's loss. A similar was decision was made in *Apache Corp v Great American Insurance Co.*[275] The fraudsters impersonated some employees of the assured's (Apache Corp) supplier and gave instructions to transfer payments to a new account which was the account of the fraudsters. The assured transferred USD$ 2.4 million. The Computer Fraud clause in the assured policy indemnified the assured for 'loss of … money… resulting directly from the use of any computer to fraudulently cause a transfer…'. It was held that the request made through emails did not meet the requirement of 'directly from the use of any computer'. The court distinguished this situation from when hackers take over the insured's computer to carry out fraudulent transfers without the involvement of an employee of the assured or any other supervening event / actions that would break the chain of causation.

3.22. In *Medidata Solutions, Inc v Federal Insurance Co*[276] and *American Tooling Center Inc v Travelers Casualty and Surety Co of America*[277] respectively where both Courts held that the

[275] No. 15-20499, 2016 WL 6090901 (5th Cir., 18 October 2016)

[276] 17-cv-2492 (2d Cir., 6 July 2018); Celso (n 273).

[277] No. 17-2014, 2018 WL 3404708 (6th Cir., 13 July 2018). The same reasoning was applied in E*rnst v. Hiscox* 23 F.4th 1195 (9th Cir. 2022). Here the 9th Circuit Court decided to not apply its their own decision: *Pestmaster Services Inc v*

involvement of employees of the assured after having been manipulated by the hackers to process the transfers are not substantial enough to break the chain of causation. As such it was the held by both courts that had it not been for the fraudulent actions of the hackers, the employees would not have made the transfers. In the latter case, the court stated that the assured suffered direct loss that was caused by the computer fraud because the hackers sent fraudulent emails which was what caused the insured to transfer the money to the hackers. In *American Tooling Center Inc*, the decision turned on the meaning given to computer fraud under the insurance policy which was defined as 'the use of the computer to fraudulently cause a transfer of money….'[278] The court construed the clause widely and denied that it was limited to acts where the hackers take control of the assured's computer. If the clause was more narrowly defined, it is likely that the decision of the court would be different but here where there is ambiguity as to the meaning of the words, they must be construed in favour of the assured.

3.23. While these cases are not binding on legal practice and interpretation in the UK, they could serve as a starting point for assured and insurers in understanding how specific computer fraud clauses have been interpreted in other jurisdictions. This is of importance since the computer and cyber insurance market in the USA is more mature than the London market. Additionally, many insurance companies in the UK have subsidiaries or offices in the USA so subject to the difference in legislation, an insurer in the UK with partners in the USA will often treat the clause similarly in the UK. It is yet to be seen how UK commercial judges will interpret 'computer fraud or social engineering' clauses. Based on the discussion of the American cases, it is evident that the courts

Travelers Casualty and Surety Co. of America No. CV 13-5039-JFW, 2014 Westlaw 3844627, page 8 (C.D. Ca. July 8, 2014); 2016 WL 4056068 (9th Cir. July 29, 2016) and *Vons Cos. v. Federal Insurance Co.*, 57 F. Supp. 2d 933, 943 (C.D. Cal. 1998), *aff'd* 212 F.3d 489 (9th Cir. 2000) because of difference of facts and insuring agreement respectively. Yet, the decision in *Ernst v Hiscox* still applied the 'direct means' test. The difference was in the treatment of the role of the employee who unknowingly acted upon the fraudsters instructions and whether their role was an intervening act so that the direct means test would not be satisfied. The Ninth Circuit court reversed the decision of the district court by stating the act of the employee was not an intervening event, thus Ernst loss was a direct result of the fraudulent instructions which was covered under the policy. These recent cases have expanded the meaning of 'direct' by treating the acts of employees who act on the fraudulent instructions as non-intervening acts which means if this trend continues more insurers will be required to cover loss from social engineering under their fraudulent funds transfer and computer fraud polices.

[278] No. 17-2014, 2018 WL 3404708 (6th Cir., 13 July 2018); Celso (n 273).

even within the same jurisdiction do not necessarily agree on how clauses should be interpreted especially where there is some involvement or manipulation of an employee of the assured. Based on the facts of the scenario, the logical approach is to adopt and apply the reasoning in Pestmaster line of cases and interpret 'directly from' as immediate and without the involvement knowingly or inadvertently of an employee or agent of the assured or any supervening event which would break the chain of causation. This should be the approach if Santos seeks compensation under any of its computer crime policies or a fraudulent transfer funds clause. There is no reason to complicate the meaning of directly from and it should not be interpreted as the proximate cause of the loss which in insurance terminology does not simply mean 'directly from'. A direct cause of loss may not be the proximate or most efficient cause of the loss. It is suggested that policies or clauses written to address social engineering loss consider the treatment of unwilling or negligent third-party intervention particularly from employees or agents and whether liability will be shifted to insurers or remain for example in this scenario with the owners of Santos.

3.24. The second set of cases focus on the 'unauthorised access' exclusion or the requirement of authorized access. These cases have been strictly interpreted and creates some difficulty for an assured whose policy on computer fraud or social engineering requires 'authorized access' or excludes 'unauthorised access'. *Taylor & Liberman v Federal Insurance Co*[279] involved the assured accounting firm which controlled the account of a client's bank account. The client's email was hacked and the fraudsters in turn emailed the assured and directed them to transfer money from the client's account to the fraudster's account. Two emails were sent to the assured, one from the client's account and the other from a spoofed email account. Under the policy, a computer fraud required that 'there is unauthorized 1) 'entry into' its computer system and 2) 'introduction of instructions' that 'propagate [d] themselves' through its computer system." The court held that the fraudsters did not gain 'unauthorised entry in the assured's computer system' since it was the client's email that the fraudsters entered and through which they gave the assured instructions. There was no introduction of instructions propagated through the insured's own computer.

[279] No. 15-56102 (9th Cir., 9 March 2017); Celso (n 273).

3.25. The Canadian case of *The Brick Warehouse LP v Chubb Insurance Company of Canada*[280] considered the decision of the court in Taylor & Lieberman, and while it is not binding authority on the Canadian court, it certainly played a persuasive role in the decision taken by the court. The facts are that fraudsters made telephone calls and then sent fraudulent emails to the employees of the assured. Within these emails, the fraudsters changed the account details to which payments are to be made to a supplier of the insured. This meant that the payment of supplier's invoices was being transferred to the account of the fraudster rather than the supplier. The insurers refused to indemnify the assured who in return sued the insurer for coverage for these losses. The policy included a clause on funds transfer fraud and included the requirement that 'the fraudulent instructions directing a financial institution to transfer, pay or deliver money or securities from any account maintained at the institution be without the insured's knowledge or consent.' The court explained that the words 'without the knowledge or consent of the insured' would apply to a scenario where the financial institution carried out a transfer under the instructions of a third party impersonating the insured. However, in this case, the court held there was no coverage because the instructions were issued by an employee who knowingly consented to the transfer. The instructions were not issued by a fraudulent third party. The court went on to explain that even though the insured's consent was obtained fraudulently, since the policy did not specify that consent meant only 'informed consent', consent obtained fraudulently met the policy requirement.

3.26. The cases of *Aqua Star (USA) Corp v Travelers Casualty and Surety Co of Am*[281] and *Universal American Corp v National Union Fire Insurance Co of Pittsburgh, PA*[282] were both decisions that considered the exclusion of coverage for loss resulting from a person with authorized access to the assured computer. In Aqua Star the exclusion clause provided that there is no coverage for 'loss … resulting directly or indirectly from the input of electronic data by a natural person having authority to enter the Insured's computer system'. The fraudster entered the email system of the assured seafood supplier and sent instructions to the assured to change the payment details for the supplier so that when transfers were made by the assured treasury manager, they

[280] 2017 ABQB 413; Celso (n 273).
[281] No. 16-35614, 2018 WL 1804338 (Ninth Cir., 17 April 2018); Celso (n 273).
[282] 25 N.Y.3d (2015) (New York Court of Appeals); Celso (n 273).

were sent instead to the fraudsters account. The assured argued that the exclusion should not apply since the employee entered the data in Bank of America computer system rather than the assured's computer as required by the clause. The court disagreed with the assured and held the 'authorized access" exclusion applied as the losses resulted from employees authorized to enter its computer system changing the wiring information and sending payments to the fraudsters account thereby fulfilling the requirement of the exclusion. A similar decision was reached in Universal American where the insured healthcare provider fraudulently entered claims for reimbursement of services they did not provide in the insured's computer. The relevant policy wording covered losses "resulting directly from the fraudulent entry of electronic data' into the computer system of the insured." The claim by the assured was rejected on the premise that the 'reasonable expectation of the average insured upon reading the policy under New York insurance law, were that the losses were excluded because the words 'fraudulent entry' only provided coverage for a violation of the integrity of the computer system through deceitful and dishonest access" which does not apply because the fraudulent content was entered by the assured's health care provider who has authorized access to the assured's computer system. Another case *City of Unalaska v. National Union*[283], also involved an employee who provided the fraudster with information resulting in the transfer of almost USD$3 million to the fraudsters account. Here the district court interpreted 'directly' by stating that the word on its own would mean immediate but when used in a phrase 'resulting directly from', a reasonable assured would expect the phrase bears the same meaning as 'proximate cause'. The proposition that the employee act broke the chain of causation was rejected. Instead, it was reasoned that the employees' actions and the resultant loss was the objective of the fraudsters' emails, ultimately following American Tooling Center and Ernst discussed above.

D. Charterers Response

a. Spear Phishing attack - An offhire event?

3.27. Since this is a charterparty agreement, the charterers perspective in terms of his response to the spear phishing attack must now be considered. Naturally, the first response of the charterer

[283] Case No. 3:21-cv-00096-SLG, 2022 WL 826501 (D. Ak. Mar. 18, 2022).

is to propose that the vessel is offhire. In deciding whether the phishing attack described herein qualifies as an offhire event which will suspend the charterers obligation to pay hire, a process needs to be followed where there is a constructive interpretation of the terms of the charter. The time charterer needs to prove that one of the specified off hire events has occurred and that due to that occurrence there has been a loss of time which also prevented the full working of the vessel.[284] The event must be fortuitous and cannot be a breach caused by the charterer. In establishing whether there has been a loss of time, the test is to determine whether the vessel is unable to perform the task that is immediately required of it. With that said, in applying the principles to these facts, the question is whether the phishing attack falls within the category of events which qualifies as an offhire event, was there a loss of time caused by its occurrence and was the vessel prevented from performing the task for which it was required at the time when the phishing attack was discovered?

3.28. The burden will be on the charterer to establish that the phishing attack is indeed an offhire event.[285] While the charterparty herein was written on NYPE 93 form, the discussion will also consider the same scenario but with the incorporation of BALTIME 1939 (Revised 2011) and SHELLTIME 3 and 4. Clause 17 of NYPE 93 recites the circumstances under which the vessel will be placed offhire. Understandably, it does not mention a spear phishing attack neither did it mention the more general term of cyber-attack. The period when this clause was drafted, cyber-attack onboard a vessel or even on facilities of the maritime sector was far-fetched, maybe even unrealistic in the minds of some stakeholders. Despite this limitation with the language used, the forms continue to be the backbone of many charter party agreements. The three major elements that will trigger the operation of the offhire clause will be discussed.

> 17. **Off Hire**
>
> **In the event of loss of time** from deficiency and/**or default** and/**or strike of officers or crew**, or deficiency of stores, fire, breakdown of, or damages to hull, machinery or equipment, grounding, detention by the arrest of the Vessel, (unless such arrest is caused by events for which the Charterers, their servants, agents or subcontractors are responsible), or detention by average accidents to the Vessel or cargo unless resulting from inherent vice, quality or defect

[284] Baris Soyer and Andrew Tettenborn (eds), *Charterparties: law, practice and emerging legal issues* (2018, Informa).
[285] *Royal Greek Government v. Minister of Transport* (1948) 82 Lloyd's Rep. 196,199 (Bucknill LJ); *The Doric Pride* [2006] 2 Lloyd's Rep. 175, 179 (Rix LJ).

of the cargo, drydocking for the purpose of examination or painting bottom, or **by any other similar cause preventing the full working of the Vessel**, **the payment of hire and overtime, if any, shall cease for the time thereby lost.** …

i. Did the spear phishing prevent the full working of the vessel?

3.29. To answer this question, we must first understand the meaning of the phrase 'preventing the full working of the vessel'.[286] Since it appears after the list of events which would trigger the clause and before the effect, it operates as a capture all or qualifying phrase. In other words, each event whether it be the deficiency and default and or strike of officers or crew, detention of the vessel, fire or damage to hull inter alia, will only qualify as an offhire event if in addition to causing the loss of time has also prevented the full working of the vessel.[287] Therefore, the spear phishing attack must have prevented the full working of the vessel. The full working of the vessel is prevented if it is not in an efficient state to perform the service required of her during the voyage. Accordingly, the question is whether Santos was in an efficient state to do what was required by the charterers when it was called upon to do so? If the response to this question is in the negative, only then will the parties consider if the phishing attack is a cause to trigger the operation of the offhire clause. In this case, there is no information of the service that the charterers required of the vessel, however if the vessel was in the middle of the journey or at the loading or discharge port when the phishing attack is discovered, it is arguable that Santos would be in an inefficient state, and this would have prevented her from continuing her journey or loading or unloading of the cargo from Santos. On the surface, this seems unreasonable, yet it is possible that the vessel is prevented from performing the service required of it by the charterer because of the vulnerabilities in the interface between the network facilities ashore and the vessel. This is a valid concern since the tracking system for cargo is usually connected to the company's onshore system and directly between the shipper and the ship.[288] In this case, where the company's system is under attack, the vessel would be in an inefficient state and would be prevented from proceeding with the unloading

[286] *The Aquacharm* [1982] 1 Lloyd's Rep. 7, 9 (Lord Denning M.R).
[287] *The Mareva A.S*. [1977] 1 Lloyd's Rep. 368, 381 (Kerr J).
[288] Bimco and others, 'The Guidelines on Cyber Security Onboard Ships: Version 4' (Annex 4, 2020) <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships> accessed 18 September 2022.

of the cargo. In the alternative if the vessel was in the middle of its voyage, the shipowners may have also found it in the best interest of all stakeholders not to proceed until they receive security clearance. In both instances the vessel has been prevented from performing the service which is required of it and therefore the charterers are within their rights if other conditions are satisfied to argue that the vessel is offhire.

3.30. Preventing the full working of the vessel has been construed to include activities not usually required by the charterer such as repairs of machinery or extinction of a fire[289]. Furthermore, the full working of a vessel may be prevented by third party interference such as piracy[290] similar to the situation described in scenario 1 above. This means that it does not need to be an internal factor or peril onboard the vessel which prevents its full working. In fact, "the vessels working may be prevented by legal as well as physical means and by outside as well as internal causes."[291] While these external factors aimed directly at the vessel will qualify as preventing its full working , the same principle is not applied when those external factors affects shipping generally even though they may cause delay or interrupt the voyage.[292] Accordingly, both internal and external factors may prevent the full working of the vessel however the external factors must be directly aimed at the vessel itself.

3.31. Webster J in the *Roachbank* proposed a more restrictive interpretation, he was of the view that preventing the full working of the vessel 'implied that there was an internal issue with the vessel itself',[293] however *Rix J* in *The Laconian Confidence* rejected this, maintaining that 'the natural meaning of the words did not allow for such restrictive interpretation'[294] and he relied on the absence of binding authority to suggest otherwise or to prevent him from arriving at that conclusion. On the contrary, the clause excludes delay in discharge of damaged cargo caused by a leakage through the defective hatch as the ship was still fully capable of carrying out the service

[289] Terence Coghlin and others, Time Charters (7th edn, Informa 2014) para 25.14; *The Clipper Sao Luis* [2000] 1 Lloyd's Rep. 645, 651.
[290] *The Saldanha* [2011] 1 Lloyd's Rep. 187.
[291] *The Laconian Confidence* [1997] 1 Lloyd's Rep. 139, 150 (Rix J); Terence Coghlin and others, Time Charters (7th edn, Informa 2014) para 25.15.
[292] Terence Coghlin and others, Time Charters (7th edn, Informa 2014) para 25.15.
[293] C.A. Venezolana De Navegacion v Bank Line (The "Roachbank") [1987] 2 Lloyd's Rep. 498, 507.
[294] The Laconian Confidence [1997] 1 Lloyd's Rep. 139, 150.

required of her including the unloading of the cargo.[295] Similarly preventing the full working of the vessel will not include any physical obstruction to navigation, therefore will not qualify as a ground on which the charterers will successfully claim that the vessel is offhire.[296] An event will only be accepted as preventing the full working of the vessel if the charterer loses the use of his vessel against his will or control.[297] Preventing the full working of the vessel will include the partial malfunction or reduction in services and not necessarily the complete disablement of the vessel. This means that the spear phishing attack will qualify as an offhire event even in circumstances where Santos is not completely dysfunctional. If the manner in which or the speed at which a service is usually done or expected to be completed has been affected due to the attack, these conditions may be enough to satisfy the operation of the offhire clause as the vessel is prevented from carrying out its services as per the terms of the contract.[298]

ii. SHELLTIME 3 & 4 and BALTIME 1939

3.32. Shelltime 3 and 4 offhire clause 21 refer to the 'efficient state of the vessel' which have been interpreted differently from 'preventing the (full) working of the vessel.

SHELLTIME 3

21. In the event of loss of time (whether arising from interruption in the performance of the vessel's service or from reduction in the speed of the performance thereof or in any other manner) …….

    hire shall cease to be due or payable **from the commencement of such loss of time until the vessel is again ready and in an efficient state to resume her service** from a position not less favourable to Charterers than that which such loss of time commenced.

SHELLTIME 4

21. (a) On each and every occasion that there is loss of time (whether by way of interruption in the vessel's service or, from reduction in the vessel's performance, or in any other manner);

[295] *The Mareva A.S.* [1977] 1 Lloyd's Rep. 368.
[296] The Laconian Confidence [1997] 1 Lloyd's Rep. 150; Terence Coghlin and others, Time Charters (7th edn, Informa 2014) para 25.13.
[297] Terence Coghlin and others, Time Charters (7th edn, Informa 2014) para 25.17.
[298] *Tynedale v. Anglo-Soviet* [1936] 1 All ER 389.

……

> (v) the vessel shall be off-hire from the commencement of such loss of time until she is again ready and in an efficient state to resume her service from a position not less favorable to Charterers than that at which such loss of time commenced; provided, however, that any service given or distance made good by the vessel whilst offhire shall be taken into account in assessing the amount to be deducted from hire.

The language used is 'until the vessel is again ready and in an efficient state' which has been interpreted as applying only to the physical condition of the vessel.[299] *Rix J* in the *Laconian Confidence* agreed that the emphasis on the efficient state of the vessel in Shelltime 3 was different from the language used in *NYPE* of 'preventing the working of the vessel'. He also accepted that restricting the clause to only physical condition as discussed by *Leggatt J* in *the Manhattan Prince*[300] based on the difference in wording was justifiable, yet this was not an approach that should be applied to the *NYPE* offhire clause.[301] Rix J expressed:

> In my judgment therefore, the qualifying phrase "preventing the full working of the vessel" does not require the vessel to be inefficient in herself. A vessel's working may be prevented by legal as well as physical means, and by outside as well as internal causes. An otherwise totally efficient ship may be prevented from working. That is the natural meaning of those words, and I do not think that there is any authority binding on me that prevents me from saying so.[302]

3.33. Having discussed the foregoing, the question is whether the spear phishing attack prevented the working of the vessel? If the charter party is written on a *NYPE* or similar wordings such as *clause 11* of *BALTIME 1939 (Revised 2011)*[303] form, there is not much difficulty. This is because the event that causes or significantly prohibits the working of the vessel can be of a legal, administrative or physical nature. The event itself can be an external factor provided it is directed at the vessel. Spear phishing is a targeted type of cyber-attack therefore the perpetrators would have selected Santos as their main or one of their targets. The main obstacle is whether a direct

[299] The Manhattan Prince, [1985] 1 Lloyd's Rep. 140, 146; The Bridgestone Maru No. 3 [1985] 2 Lloyd's Rep. 62, 83.
[300] Ibid The Manhattan Prince.
[301] The Laconian Confidence [1997] 1 Lloyd's Rep. 139, 150.
[302] Ibid.
[303] Clause 11(a) of BALTIME 1939 (Revised 2001) Uniform Time Charter with a minor variation 'either hindering or preventing the working of the vessel and continuing for more than 24 consecutive hours' carries the same meaning as clause 17 of NYPE 93 'preventing the full working of the vessel'.

attack on the parent company would also qualify as a direct attack on the vessel? If this is the case, it would be a challenge for the charterers to prove that it was the vessel itself that was attacked in order to qualify as an offhire event. The charterers would have had to have insider knowledge about the IT and OT of the company, the existing vulnerabilities and access to data showing the most recent cyber-attacks on the system including both the successful and failed attacks. As noted above, the spear phishing does not need to fully disable the operation of the vessel, it is enough if there is a malfunction or substandard operation of a particular aspect of the vessel due to the attack. Even if the spear phishing attack will be challenged as not being the type of external event envisioned by the drafters, it is possible that an attack of this nature may fit perfectly well into the administrative category of events mentioned in the judgement of Rix J in the *Laconian Confidence*. In fact, it was weaknesses in the administration or overseeing of the security of email exchanges between the owners and charterers which caused this type of breach to occur.

3.34. Conversely if the charterparty incorporates a SHELLTIME *3* or *4* form, with the words 'efficient state of the vessel', this entails a more restrictive meaning where the event or cause must be related to the physical condition and internal to the vessel itself. The question remains will a cyber-attack which targets the parent company but also affects the vessel qualify as an 'physical internal cause' that may affect the 'efficient state of the vessel'? The spear phishing attack is not a mechanical issue, it is not a problem with the hull, navigation or communication system of the vessel itself. It is caused by a malicious third party whose intention it was to steal and divert funds that was sent by charterers intending for it to be deposited to the ship owners accounts. By the narrow interpretation to which the cases have given to the 'efficient state of the vessel', it is unlikely that the courts or arbitrators will extend its meaning to include cyber-attacks of this nature especially where there is no physical damage to the vessel itself. Consequently, charterers may not be able to rely on the spear phishing attack or any cyber related attack to initiate a claim for an offhire clause to become operational or rather to withhold their hire on the basis.

b. Can the spear phishing qualify under a named offhire event?

If the full working of the vessel has been prevented by the spear phishing attack, the next task is to consider whether the attack fits under any of the named events that would trigger the operation of the clause.

i. Deficiency and or default and or strike of officers or crew

3.35. The circumstances under which Santos became a successful target to the spear phishing may be categorized as negligence or default on the part of the corporate management team. The BIMCO Guidelines clearly identify as vulnerabilities 'shipboard computer networks which lack boundary protection measures and segmentation of networks.'[304] Therefore if the network onboard a vessel is not kept secure and separate from that of onshore facilities, any damage resulting therefrom will be due to the disregard for the guidelines and best practices as recommended by industry specific organisations. This would also amount to a non-compliance with the January 2021 deadline which required shipowners and managers to incorporate cyber risks into their safety management systems in accordance with *IMO Resolution MSC.428 (98)*. Despite the apparent disregard for best practices or negligence or default on the part of officers or crew, such inaction or omission will not qualify under clause 17 as 'deficiency and or default of officers or crew'. Justification for this can be found in the case law pertinent to the interpretation of clause 17 NYPE such as *The Saldanha* (clause 15 of the charterparty)[305] where 'default' was not taken to include negligence even though it was naturally expected to do so. Default means the refusal by officers or crew to perform all, or part of their duties owed to the shipowner and not the negligent performance of those duties.[306]

[304] Bimco and others, 'The Guidelines on Cyber Security Onboard Ships: Version 4' (Annex 4, 2020) 3, 17, 19-20, 34 <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships> accessed 16 February 2022

[305] [2011] 1 Lloyd's Rep. 187.

[306] Ibid [21] and [28].

ii. **Any other (similar) cause preventing the full working of the vessel**

3.37. This catch all clause is likely to become the most relied on ground for the charterers who are seeking to place the vessel offhire due to the vulnerabilities arising from a spear phishing attack. Notwithstanding the use of the word 'any' which gives the impression of a limitless application, the clause itself is interpreted and its scope limited by the other qualifying events in Clause 17. The ejusdem generis rule imposes this type of restrictive application, thus 'any other cause' will only include those which are similar to the events already mentioned. The amended NYPE 93 added the word 'similar', so the clause reads 'any other similar cause…' which dispels any ambiguity or the need for debate as occurred in cases which incorporated NYPE 46. The issue was discussed in *the Laconian Confidence* by Rix J who said "'any other cause' without 'whatsoever' relates only to the physical condition or efficiency of the vessel or crew and or cargo".[307] *The Laconian Confidence* was delayed primarily due to the decisions taken by the port authorities at Chittagong in Bangladesh. The court rejected the charterers claim and held that the vessel remained on hire as it was never intended that a standard offhire clause should make the shipowner liable for delay caused by port authorities especially when their action is not a reasonably foreseeable consequence of any named cause.[308] The cause itself need not be physical, it can be legal or administrative actions but must be related to the physical condition or the efficiency of the vessel.[309] In *Court Line* v. *Dant & Russell Inc*[310] the boom was not a cause related to the physical condition of the vessel rather it was deliberately created by the Chinese to prevent the Japanese from entering the area. As such the obstruction to the river by the boom was not a cause that fell within the category of 'other causes' and even though there was a delay and loss of time, the Errington Court vessel was still on hire. The Errington Court was fully functional and, in a state, to carry out any task required of her.

3.38. Based on this analysis, even if the spear phishing attack is deemed to have prevented the full working of Santos, the spear phishing attack will not qualify under any of the named offhire

[307] *The Laconian Confidence* [1997] 1 Lloyd's Rep. 139, 150.
[308] ibid 139, 151.
[309] Terence Coghlin and others, Time Charters (7th edn, Informa 2014) para 25.39.
[310] [1939] 3 All ER 314, 318 (Branson J).

events in NYPE nor will it qualify as 'any other cause' since it is unlikely that a spear phishing attack will be related to the physical condition or efficiency of the vessel. What exactly does the physical condition or efficiency of the vessel (including the crew), or cargo mean? There is a difference between default and efficiency of the crew, the latter would include the smooth uninterrupted effort of the crew where they achieve each task with maximum productivity and minimal time wasting. The effect of the spear phishing attack on the vessel is exactly as described, it has hindered or prevented the crew from maximum productivity. The entire vessel is at a standstill, sailing is prohibited and all devices onboard are switched off including the cargo management system so even if the charterers instructions were to unload the cargo, this would be prevented in fear of further penetration by the cyber hackers who could continue to exploit the security weaknesses for their own benefit and at the detriment of the shipowners, managers, charterers and other stakeholders who have an interest in the time charter. Despite the clear interconnection between the spear phishing attack and the loss of time or delay to the charter, the emphasis placed on the event to be related to the physical condition of the vessel remains a challenge.

3.39. Conversely, if the clause read 'any other cause whatsoever' as would be found in an amended NYPE form and distinguished by Rix J in the *Laconian Confidence*, the interpretation changes as ejusdem generis rule will no longer apply. Therefore, the causes that will qualify as an offhire event need not be related to the physical condition or efficiency of the vessel or crew. Accordingly, causes such as the boom in a river and the interference of the port authority satisfies this test and there is nothing within these examples to suggest the spear phishing attack herein may not equally qualify as any other clause whatsoever. *The Mastro Giorgis*[311] illustrates this; the charter was to transport grain from Argentina to Italy and to unload some in Baretta. Upon arrival in Baretta, the cargo was found to be damaged, and the retrievers arrested the vessel for few days. *Lloyd J*, held that 'where an offhire clause includes the word 'whatsoever', any cause will suffice as an offhire event whether it be physical or legal, the only question being whether the said cause prevented the full working of the vessel for the service immediately required.'[312] Without doubt

[311] [1983] 2 Lloyd's *Rep. 66.*
[312] The Mastro Giorgis [1983] 2 Lloyd's Rep. 66, 68-69.

spear phishing attack cannot be discarded under this wording provided the charters can establish the causal link between the spear phishing and it preventing the full working of the vessel for the service immediately required of her. Any suggestion that 'any other cause whatsoever' should be limited only to a physical or legal cause should be dismissed based on the statement of Lloyd J as it would run counter to the expansive approach adopted by previous cases in giving meaning to the more restrictive clause 'any other cause'. Since 'any other cause' includes physical, legal and administrative causes, it would be nonsensical to apply a more restrictive interpretation to 'any cause whatsoever' to mean any cause of a legal or physical nature but excluding administrative. The better approach is to treat 'any other cause whatsoever' to mean any cause in the literal meaning of the word 'any', the only condition being that the identified cause must be directly linked or have prevented the full working of the vessel for the service immediately required of her.

3.40. This expansive approach is to be applied to the BALTIME 1939 (Revised 2001) form where clause 11(a) made reference to 'or other accident, 'either hindering or preventing the working of the vessel and continuing for more than 24 consecutive hours'.[313] *Mocatta J* in *The Apollonius*[314] applied this approach and by so doing agreed with the judgment of Lord Justice Atkin in *Magnhild v. McIntyre* who expressed that 'The words "other accident" are words of large import'[315]. *Mocatta J* explained that the circumstances under which the vessel bottom became dirty contributed to slow steaming and the loss of time was in fact an 'accident' in the normal meaning of the word and as interpreted in previous cases. He explained that the thick layer formed by molluscs at the bottom of the vessel was something that occurred unexpectedly and out of the ordinary course of things as the location at which the vessel was staying for a lengthy period of time is fresh water and molluscs are more commonly found in salt water. Based on the meaning given to the words 'other accidents' in previous cases, *Mocatta J* had no difficulty in holding that 'any other accident' is wide enough to include the fouling of the bottom of the ship in those circumstances. This prevented the efficient working of the vessel since her speed had been reduced

[313] Roskill J, *Court Line, Ltd. v. Finelvet, A.G. (The "Jevington Court") [*1966] 1 Lloyds Rep 683, 698.
[314] *Cosmos Bulk Transport Inc v China National Foreign Trade Transportation Corporation (The "Apollonius")* [1978] Lloyd's Rep. 53, 65.
[315] (1921) 6 Ll.L. Rep. 190; [1921] 2 K.B. 97, 107.

to levels below that which she would otherwise be capable of, therefore hire was not payable for the 4.821 days lost.[316]

3.41. Certainly, this wide meaning is warranted but it is difficult to imagine that it was the intention of the drafters to cover any event or circumstance which causes a loss of time. If so, the potential loss to the shipowner will be extensive with the only control mechanisms being the requirement that the event causing the loss persists for at least 24 hours and either hindered or prevented the full working of the vessel. Considering the foregoing, will the spear phishing attack fit into 'any other accident'? If a boom in a river and encrustation of a ship's bottom qualifies under this cause, a spear phishing attack under these circumstances may also qualify provided it causes a loss of time which persists for at least 24 hours. The only foreseeable problem may be that the event causing the loss, that is the spear phishing must be an accident. As previously mentioned, an incident will be classified as an accident if there is an element of uncertainty and the absence of intent. Accordingly, the charterers may experience difficulties proving that the spear phishing attack was an accident. The perpetrators deliberately and intentionally targeted Santos with the aim of fraudulently diverting funds thereby it is not an accident. However, despite this seemingly logical approach, decisions such as *Court Line v Dant Russel*[317] will be called into question since the boom was deliberately created by the Chinese and so would not be an accident thus would not qualify under an offhire clause containing the words 'any other accident'.

3.42. What if the charterparty included a clause similar to clause 101 that was discussed in London Arbitration 25 /19? The clause provides:

> **Health and Safety**
>
> The Vessel will comply with any and all safety regulations applicable during the currency of this Charter Party including those in effect at any port of loading and or discharge. If the Vessel does not comply with said safety regulations or requirements, the Vessel will be off-hire until the Vessel is compliant with said safety regulation or requirements, the Owners will take

[316] *Cosmos Bulk Transport Inc v China National Foreign Trade Transportation Corporation (The "Apollonius")* [1978] Lloyd's Rep. 53, 66.
[317] [1939] 3 All ER 314.

> immediate corrective steps and any stevedores standby time and other expenses involved are to be for Owners' account. [318]

The incorporation of this or any clause with similar wording would answer some of the questions relating to cyber-security risk management and offhire clauses. The vessel must not only comply with what can be properly classified as safety regulations, but the compliance obligation extends even to safety requirements thereby covering industry guidelines and codes published by international organizations, class societies and specific requirements at the ports of loading and discharge and not necessarily only regulations created by flag states / government. The Arbitrator held that the Pacific Coast Marine Safety Code which governed the contractual terms between the stevedores and their members union is a safety requirement and possibly regulation within the meaning of terms as used in the clause. In addition to the safety regulations and requirements of the flag state, the vessel must also comply with the safety regulation and requirements at both the port of loading and discharge which are applicable during the currency of the charter-party. If the vessel was noncompliant with any safety regulation or requirement, it will be offhire until the owner takes immediate corrective measures and any expense incurred will be the responsibility of the shipowner. In London Arbitration 25/19, the stevedores refused to work until the cranes were fixed as they failed gear inspection. While these physical malfunctions will continue to plague the shipping industry, so too more vessels will fail classification society inspections based on their vulnerabilities and or their flouting of cybersecurity guidelines and regulations. As discussed above, it is the shipowner /master who is responsible for the safety and navigation of the vessel, so it is only right that the vessel will be deemed offhire when it fails to meet cybersecurity regulations and requirements that are current during the period of the charterparty.

3.43. In light of the collective efforts by Governments, the IMO, ports and other stakeholders within the marine sector, if a charterparty does not include a clause which addresses cyber risks as an offhire event, it is prudent to imply an indemnification to the charterers where the shipowners have failed to implement and or show recorded evidence of cybersecurity procedures and as a result there is a loss of time. Based on London Arbitration 25/19, the best practice is to declare that the vessel must comply with cybersecurity regulations including or excluding safety requirements.

[318] Lloyds Maritime Law Newsletter, 'London Arbitration 25/19' (07 November 2019, Informa).

If during the currency of a charter, the regulatory and cyber-security requirements at for example the loading or discharge port changes, will the vessel be denied entry to the port or risk losing their insurance coverage for changes made during the voyage? One side of the argument is that the HVR should be applied and since this would be a risk that affects the seaworthiness of the vessel, the requirement to meet the obligations under security regulations and guidelines would be limited to the regulatory requirements at each location before and at the start of the voyage. Conversely, others may think that the vessel must meet these requirements throughout the voyage and if there are stages, at each stage of the voyage the requisite steps must be taken to ensure the vessel is cyber compliant based on state regulations before it enters the territorial waters of that state and also ensure that the specific cyber security requirement of each port is satisfied. This approach requires high levels of cooperation and communication between personnel ashore for example between and among the Designated Persons ashore, CYSO, masters, government agencies and port authorities.

II. Insurance Implications of the spear phishing attack

3.44. The fraudulent transfer or diversion of funds is not a new phenomenon however the proliferation and increasing dependence on technology within the marine sector has also led or contributed to surges in the number of fraudulent transfers. The circumstances herein are no different and are examples of the vulnerabilities in payment systems generally which also affects the marine industry particularly transactions between shipowners and charterers. The conditions under which the funds were stolen have already been disclosed and the arguments put forward by the shipowners and charterers in pursuit of being compensated for liabilities arising therefrom. An area of concern for the charterers and shipowners whenever there is a conflict is the possible response of their insurers. Ideally, each party would expect that their insurer will be willing to cover the cost or liability incurred as a result of the spear phishing attack, naturally however there will also be apprehension as to whether insurers will accept liability in these circumstances where the cause of the loss is due to a cyber-attack.

The discussion in this section will be divided into two sections, the first will look at the marine insurance policies that usually cover loss of hire to examine how those insurers would respond and

then secondly identify cyber insurance policies to see whether they will address these risks and liabilities.

A. Loss of Hire Insurance (LOH)

3.45. The spear phishing attack has caused considerable delay to the time charter. Section 55 (2) (b) of the MIA 1906 provides that unless the insurance policy provides otherwise, the insurer will not be liable for any loss proximately caused by delay, even though the delay may be caused by a peril insured against. This provision highlights the attitude and reservation of insurers to accept responsibility for losses proximately caused by the delay. For this reason, loss of hire is not provided for in the traditional marine insurance policies and those cargo or freight policies which incorporate similar wording. So, the shipowner would only be able to recover the amount lost in hire if he had a LOH insurance or had this cover as an extension of for example his hull insurance. Whereas the London market is known worldwide for its command of the marine insurance market, the same is not true for LOH insurance. Instead, LOH is commonly purchased from the Nordic Market even though there are some UK insurers who offer such coverage protection. The insurance is based on the Nordic Plan 2013, version 2016. For those purchasing LOH in the London market in addition to the option of purchasing from an insurer such as Gard whose policy is based on the Nordic Plan, there is also the Loss of Charter Hire Insurance Including War (ABS 1/10/83) and Loss of Charter Hire Insurance Excluding War (ABS 1/10/83) which are widely used in the market. Both the Nordic plan as offered by Gard Marine and Energy and the A.BS 1/10/83 will be analysed in relation to the spear phishing attack and the losses experienced by both the shipowner and the charterers.

3.46. Traditionally LOH insurance covers the assured for loss of income resulting from damage to the vessel, the damage must be of the type that is recoverable under the vessel's hull insurance.[319] In describing the scope of the policy, there are already obvious problems that will arise when an attempt is made to recover losses which do not have any link with a physical damage

[319] Handbook on Loss of Hire Insurance: Norwegian Hull Club (para 2-3-2) <https://www.norclub.com/handbook-on-loss-of-hire-insurance/> accessed 18 September 2020.

to the hull of the vessel. LOH insurance usually only reimburse the shipowner for hire if as a result of damage to the hull or machinery of the vessel covered under a H&M or H&M war policy, the payment of hire is suspended.

a. ABS 1/10/ 83

3.47. The clause begins by stating that the insurance is subject to English law and practice. It goes on to explain in clause 1 (a) and (b) the circumstances or events which will trigger the operation of the clause. Clause a and b will be discussed in alternate order.

> 1. **If in consequence of any of the following events**:
>
> (a) loss, damage or occurrence covered by Institute Time Clauses-Hulls (1/10/83) or Norwegian Hull Form or American Institute Hull Clauses (2nd June 1977) and also loss damage or occurrence covered by Institute War and Strikes Clauses-Hulls (1/10/83) or American Institute Hull War and Strikes Clauses (1/12/77) plus Addenda 1 and 2, (Option of clause to be exercised at inception)
>
> (b) breakdown of machinery, including electrical machinery or boilers, provided that such breakdown has not resulted from wear and tear or want of due diligence by the Assured, occurring during the period of this insurance the Vessel is prevented from earning hire for a period in excess of ……days in respect of any accident, then this insurance shall pay……. of the sum hereby insured for each 24 hours after the expiration of the said days during which the Vessel is so prevented from earning hire for not exceeding a further …….. days in respect of any one accident or occurrence (and not exceeding ……. days in all during the currency of this Insurance (irrespective of the expiry date of this insurance)) provided that the repairs in respect of which a claim is made hereunder are completed within 12 months of the expiry of the period covered by this policy.

Reference to loss, damage or occurrence covered by the Institute Time Clauses Hull or covered by the Institute War and Strikes Clauses -Hull or the Norwegian Hull Form is an indication of the interconnection between claim for LOH and a claim under a Hull Form. For this discussion, we will assume that the underlying hull clause is the ITCH 83. This means that the types of losses covered by clause 1 (a) of the ABS 1/10/83 are those listed in for example clause 6 of the ITCH 83. It only makes sense for the same exclusions in the ITHC 83 to apply as well under ABS form. The same discussion in scenario 1 as it relates to cyber risk and whether hull insurers will cover those risk will apply here obviously taking into consideration the commonly used cyber exclusion clause CL.380. The conclusion from those discussions is that traditional hull insurance including

the ITCH 83 does not adequately protect the assured against cyber risk particularly those risks that do not result in the physical loss of or damage to the vessel itself. Furthermore, most hull policies have expressly excluded cyber risk, therefore in most instances the assured would need to buyback cyber coverage through an endorsement clause from their hull insurer or choose to purchase a cyber insurance policy designed specifically to cover the perils unique to cyber risks. The problem remains the same with the spear phishing attack, it will not qualify or fit under any of the named perils in the ITCH 83 or any of the newer versions of the form since there has been no physical loss or damage to Santos.

3.48. Despite the interconnection between the hull and loss of hire insurance policies, there is doubt as to whether there really is a requirement for the vessel to be physically damaged before a loss of hire insurer will be engaged in the conversation as to liabilities. The uncertainty surrounding this issue was revived after the decision of the Court of Appeal in "Wondrous"[320]. The case concerns a charterparty where the owners let their vessel *Wondrous* to the charterers**,** *Dr Mojtaba M Tehrani of Barter International Co of Tehran* for the carriage of molasses from Bandar Abbass to one or two ports in Northern Europe or the Mediterranean. It was agreed that 50% of the freight was payable on signing bills of lading and balance before breaking the bulk at the discharge port. Another term of the charterparty is that freight was payable discountless and nonreturnable whether the vessel is lost or not. The vessel took over a year to complete loading and by this time, the machine became inoperable and had to be repaired. The owners suffered huge losses and made claims under both their loss of hire and freight policies issued by the defendant underwriters. For the purposes of this discussion, we will focus on the claim under the loss of hire policy. The policy provided that the insurers would only pay if in consequences of the risks enumerated in the *Institute War and Strike Clauses Hulls – Time 83* the vessel was prevented from earning hire or reward. The Defendants were not convinced that the plaintiff suffered any losses under the loss of hire policy. Hobbhouse J decided that the vessel was in fact deprived of her earning capacity, however it was the customs regulation at Bandar Abbass which made it illegal to sail as they were without

[320] *Ikerigi Compania Naviera S.A and Others v Palmer and Others Global Transeas Corporation and Another v Palmer (The "Wondrous")* [1992] 2 Lloyds Rep 566.

a customs clearance. The plaintiffs fail to establish their claim under the loss of hire insurance so they could not recover.

3.49. Unsurprisingly, the plaintiffs made an appeal to the Court of Appeal. The relevant issue is whether the policy covers loss of hire irrespective of loss of or damage to the vessel? Hobbhouse J in the lower court was of the view that loss of or damage to the vessel is not a prerequisite for recovery of loss of hire as loss or damage to the vessel is germane to a hull policy but not a loss of hire policy. Lloyd LJ did not agree with this reasoning and instead held that the loss of hire insurance was created to fill the gap of the hull policy, namely the inability of the assured to recover for loss of earning when the hull has been damaged and has to be repaired. So, for this reason loss of or damage to the vessel is germane to a loss of hire policy. However, the parties if they so intend, may give the loss of hire policy wider meaning than the hull policy so that loss of hire will be recoverable irrespective of loss or damage to the vessel.[321] Was this the intention of the plaintiffs in *Wondrous*? Lloyd LJ said no and relied on two points to support his stance. The first point is that if the plaintiffs had intended to cover loss of hire / earning irrespective of loss or damage to the vessel, they would have referred directly to the perils rather than beginning with the clause with the qualifying words 'if in the consequence of loss or damage to the vessel…" Furthermore, the parties could have chosen to include the freight clauses rather than the hull as the former would also include hire. Since the parties chose to include the hull policy it would make commercial sense for recovery of loss of hire to be allowed only when there has been loss of or damage to the vessel.

3.50. The second point made by Lloyd LJ is that the risks are made subject to the exclusions in clause 4 of the *Institute War and Strikes Clauses Hull* and he also referred to provisos (a) and (c), the latter provided that repairs if actually carried out in respect of damage are to be completed within 12 months of the expiry of the policy. Lloyd LJ contended that this proviso shows that the parties contemplated loss of hire resulting from damage to the vessel, therefore the need for repair is the primary or only circumstance under which cover is afforded by the policy. Accordingly, it

[321] *Ikerigi Compania Naviera S.A and Others v Palmer and Others Global Transeas Corporation and Another v Palmer (The "Wondrous")* [1992] 2 Lloyds Rep 566, 572.

was held 'that the parties deliberately chose the Hulls Clauses rather than the Freight Clauses, and that their purpose was to confine the loss of hire policy to loss of hire resulting from loss of or damage to the vessel.'[322] The case supports and is sometimes cited as the main authority for there to be damage to the hull of a vessel before an assured will be allowed to recover loss of hire. Is this really the position under the ABS 1/10/83 form? Paul Silver in his speech as Chairman of the Association of Average Adjusters 2012 focused on whether the ABS Loss of Charter Hire Insurance is still fit for purpose, disagrees with the viewpoint that a loss or damage to the vessel is germane to loss of hire policies. In fact, he emphasized the distinction between the wording of the brokers policy in Wondrous and that of the ABS 1.10.83 form. The brokers policy stated:

> …. This policy only pay if in consequence of the risks enumerated in the Institute War and Strikes Clauses Hulls – Time 1.10.83" …" the vessel or craft be prevented from earning hire…" Clause 1 of the Institute War and Strikes Clauses Hulls – Time 1.10.83 stated that " this insurance covers loss or damage to the vessel caused by…[323]

While the ABS form Clause 1 begins with

> If in consequence of any of the following events (a) loss, damage or occurrence covered by… (b) breakdown of machinery, including electrical machinery or boilers, provided such breakdown has not resulted from wear and tear or want of due diligence by the Assured...[324]

3.51. In analysing the terms of both policies, Paul Silver referred to a paper written by Mr. G.D. Kemp who he described as 'a respected marine insurance broker who wrote for the Chartered Insurance Institute in 1963' who made the point that the word occurrence is added to Clause 1 of the ABS form to cover situations such as a general average deviation to a port of refuge which does not include loss or damage of the vessel. G.D Kemp said:

> One would think that loss or damage may be sufficient but what about a general average deviation to a Port of Refuge This is why the word "occurrence" is added and I think this is probably one of the only places in marine insurance that the word is used.[325]

---

[322] ibid, 573.

[323] Paul Silver, 'Stuck in the doldrums? A consideration of whether the ABS Loss of Charter Hire Insurance wording is still fir for purpose' (The Association of Average Adjusters Chairman's Address, 10 May 2012), page 5. < https://docshare.tips/aaa-chairmans-address-on-loh_587ee6a3b6d87fb5398b58f4.html > accessed 18 September 2022.

[324] Ibid 7.

[325] Ibid.

So, the addition of the word 'occurrence' is important, however as pointed out by Silver its meaning was not explained and it is unclear whether there was a discussion on its importance.[326] Silver also highlighted the work of Geoffrey Hudson, a past chairman of the Association who wrote a paper with the title "Claims on Loss of Earning Insurances". In relation to clause 1 of the 1971 ABS wording which is similar to the 1983 version, he wrote:

> "Provided time is lost thereby, an "occurrence" covered by the stated forms of the hull policy will found a claim, even though no damage be sustained to the ship and no repairs are required. Thus if a ship runs aground and is put off-hire, time begins to run against the Loe insurers. And, of course, if after the ship is refloated, it is found that she is in need of repairs, the time lost in effecting those repairs may be aggregated with the time lost whilst aground in computing the total period in respect of which the indemnity is payable."[327]

After presenting the state of the law from the perspective of the broker and former chairman, Silver concluded by stating that 'the London market has always anticipated situations in which the vessel might not be damaged, but time has been loss and the vessel is prevented from earning. In that case, 'loss of earning would be payable as a result of there being a casualty covered as an insured peril under the relevant hull or war policy.'[328] He also decided that the wording of the brokers policy in Wondrous, particularly reference to 'any one occurrence' had a more restrictive meaning than that given to 'any occurrence in the ABS 1.10.83 form in that the former is dependent on there being a loss or damage to the vessel which is not the same for the latter form. Therefore, the decision in Wondrous is based in this restrictive interpretation, thus the judgment may not be authority for the principle that there must be loss or damage to the vessel before loss of hire can be claimed under the ABS policy. However, Silver was cautious enough to implore assureds and brokers to remove any ambiguity by making it very clear in the policy wording whether loss or damage to the vessel is a prerequisite to loss of hire claim.[329]

---

[326] Paul Silver (n 323).

[327] Paul Silver, 'Stuck in the doldrums? A consideration of whether the ABS Loss of Charter Hire Insurance wording is still fir for purpose' (The Association of Average Adjusters Chairman's Address, 10 May 2012), page 6. < https://docshare.tips/aaa-chairmans-address-on-loh_587ee6a3b6d87fb5398b58f4.html > accessed 10 April 2022.

[328] Ibid 7.

[329] Ibid.

3.52. Even if there was loss or damage to the vessel as a result of the negligence of the master, crew or pilots the assured may still encounter difficulties when seeking an indemnity from their insurer if the loss or damage resulted from a want of due diligence by the assured, owners or managers. Compare this to ITCH 95, the proviso found at the end of clause 6.2.5 apply only to the perils in 6.2.1 – 6.2.5 but now wide enough to consider and exclude any loss caused by lack of due diligence of superintendents or any onshore management. This brings into perspective the facts of this scenario, while it might be impossible to guarantee full proof security against cyber risk, it can be inferred from the facts that the phishing attack and the losses resulting therefrom are primarily due to onshore management failure to exercise due diligence in ensuring that employees are properly trained to detect signs of fraudulent emails and follow best practices at least to the level of those recommended by the experts both within the marine industry and those in cyber security management. So, the assured claim is likely to fail if it was solely dependent on a peril in clause 6.2 of ITCH 95. However, in practice this outcome is not absolute since when ITCH 95 form is used, the proviso in clause 6.2 is often modified to reflect the narrower position in ITCH 83 where due diligence is limited to assured, owners and managers.[330]

b. What is the charterer's option under the Nordic Plan?

3.53. The Norwegian Hull Club Handbook seeks to explain the correlation between the Nordic Loss of Hire Insurance and hull insurance. Part 2-3-2 of the handbook explains that loss of hire and damage to the vessel are not necessarily connected as the assured may suffer loss of income in many other ways besides damage to the vessel such as the impact of natural disasters or even strikes or congestions within ports. Nonetheless, there remains a link between hull and loss of hire insurance because 'it was believed that the extensive years of experience of the hull insurer meant that they established a right balance between what should be covered and what should be excepted

[330]Andrew Paton, 'Hull Clauses and Claims - time for some marriage counselling?' (The Association of Average Adjusters Chairman's Address, 12 May 2016) 9 <https://issuu.com/assocavgadj/docs/association_of_average_adjusters_an> accessed 18 September 2022.

from the cover'[331]. Yet, there has been no independent research into what the right balance is between the assured and the insurer as it relates to loss of hire insurance.[332] It is absurd to think that a wholesale application of the same perils and exemptions as found in hull insurance will apply to loss of hire policies. The difference in the subject matter insured is the first indication that the philosophy behind the creation of the policies is different, so what is deemed as the right balance in hull insurance may not be the right balance in loss of hire policies. In both the Nordic Plan and the English ABS 1.10.83 loss of hire policies, damage to the vessel is an essential principle. Yet, the Nordic Plan distinguishes itself from the ABS policy by clearly listing the circumstances where damage to the vessel is not necessary. Furthermore, clause 16-1 allows the assured to claim for loss of hire even if the damage is not caused by a peril covered under the plan provided the damage is one that is covered under the assured's hull insurance with the exception of total or constructive total loss which are not recoverable under the loss of hire insurance. Any damage which would have been recoverable under the plan but for the agreed deductible is also recoverable under the loss of hire insurance. The conditions of the Nordic Plan will be examined in relation to the spear phishing attack and whether the claim for loss of hire by the shipowners is recoverable from the insurer who have written his policy based on this plan specifically part one (1) and chapter 16.

Clause 16-1 reads:

> The insurance covers loss due to the ship being **wholly or partially deprived of income** as a consequence of damage to the ship which is recoverable under the conditions of the Plan, or which would have been recoverable if no deductible had been agreed, see Cl. 12-18. If the hull insurance has been effected on conditions other than those of the Plan, and these conditions have been accepted in writing by the insurer, the rules in Chapter 10-12 of the Plan shall be replaced by the corresponding conditions of the insurance concerned when assessing whether the damage is recoverable.
> The insurance also covers loss due to the ship being wholly or partially deprived of income:
> a. because it has stranded
> b. because it is prevented by physical obstruction (other than ice) from leaving a port or a similar limited area, or
> c. as a consequence of measures taken to salvage or remove damaged cargo, or

[331]Haakon Stang Lund, 'Handbook on Loss of Hire Insurance' (Norwegian Hull Club, 3rd edn. 2016) Part 2-3-2 <https://www.norclub.com/casualty-response/loss-of-hire?a=Introduction> accessed 18 September 2022.
[332] Ibid.

d. as a consequence of an event that is allowed in general average pursuant to the 1994 York- Antwerp Rules.[333]

i. Damage to the vessel

3.54. The uncertainty surrounding whether loss or damage of the vessel is required before a loss of hire claim is payable has been clarified in the Nordic Plan. Under the Nordic Marine Insurance Plan of 2013, (Version 2019) chapter 16 (1), there are 4 situations where the assured may recover loss of hire even though there was no damage to the vessel. The four situations are where the vessel is stranded, prevented by physical obstruction from leaving a port or similar limited area, as a consequence of measures taken to salvage or remove damaged cargo or due to a general average event pursuant to the 1994 York- Antwerp Rules. Any event which falls outside any of the 4 situations in Clause 16 -1a to d, will not qualify as a loss of hire event if loss of income was not a consequence of damage to the vessel itself. In other words, there must be a causal link between the damage to the vessel and the loss of income which has triggered the operation of the policy. The damage required is physical damage to the vessel that is recoverable under the Plan or the vessel's hull insurance. The question therefore is whether the spear phishing attack falls into one of the four situations named in clause 16-1a to d. An in-depth analysis is superfluous since it is obvious that the spear phishing attack and the circumstances under which Santos is prevented from working does not fit in any of the categories ranging from clause 16 –1a to d which means that even if the assureds had a LOH policy written on the Nordic Plan, they would not be able to recover for the loss of hire caused by the spear phishing attack. There was no physical damage to Santos and the spear phishing or cyber-attack generally does not fall within the named perils for which loss of hire is recoverable even when there is no physical damage to the vessel. The fraudulent transfer of hire / loss of hire is not a general average act. It is not an extraordinary sacrifice or expenditure intentionally or reasonably made or incurred for the common safety for the preservation of the vessel, cargo or hire in accordance with Rule A of the York Antwerp Rules 1994.

[333] The Nordic Association of Marine Insurers and others, 'The Nordic Marine Insurance Plan of 2013, Version 2019' <http://www.nordicplan.org/The-Plan/Part-Three/Chapter-16/#Clause-16-1> accessed 18 September 2022.

ii. Loss of Income

3.55. What constitutes loss of income was illustrated in the Capricorn[334] where the principle was laid down that if the vessel would have been unable to earn freight regardless of it being damaged, loss of income would not be recoverable under the loss of hire insurance. The plaintiff are the owners of a reefer vessel and claimed for 60 days loss of time from their loss of hire insurers. The policy incorporated the Institute Time Clauses (Hull) 1.10.83 the Norwegian "General Conditions for Loss of Charter Hire Insurance (1972) with the 1977 amendments. The reefer market was predominantly seasonal with the peak period being the first 5 months of each year and then the off season lasting from around end of May to October. During the off season, hire rates would be very low and it was typical for many owners to lay up their vessels during that period. The vessel was damaged due to the negligence of the crew, which was an insured peril. The crankshaft was quickly replaced however repairs to the generator were done between June 6 and October 7, 1986, while the vessel was in lay-up. The plaintiffs found it irrelevant to consider what use they might have made of the vessel after the end of the peak season if the vessel was not damaged. Instead, the plaintiffs' submitted that they should be indemnified for their loss based on their earning capacity 'without proof that such capacity would have been deployed by them in the market'[335]. In other words, the subject matter of the policy as submitted by the plaintiffs is. the physical earning capacity of the vessel thus so long as the vessel is physically deprived of its earning capacity, the insurers should pay for the loss of income.

3.56. The Defendant disagreed, they argued that the policy should not cover losses which the vessel would have incurred with or without damage as she would have been off the market, and she was due to be and would have been laid up throughout the low season and so the plaintiffs had no insurable interest. They also contended that if the plaintiffs were really interested in trading, they would have arranged for the vessel to trade with a portable generator while repairs are done to the damage generator by using a riding crew or at some other convenient time. This argument was used to support their case that the Plaintiffs had no intention of for the vessel to trade after

[334] *Cepheus Shipping Corporation v Guardian Royal Exchange Assurance* [1995] 1 Lloyds Rep 622.
[335] *Cepheus Shipping Corporation v Guardian Royal Exchange Assurance* [1995] 1 Lloyds Rep 622, 627.

May 31, 1986, and therefore the vessel was not 'wholly or partly deprived of her earning capacity.[336] Mance J decided that the loss of earning was not due to the damage which the vessel sustained but was because the vessel would have been out of the market anyway. Furthermore, the fact that the plaintiffs reserved a lay berth in mid May 1986 is either clear indication that they had no intention of exercising their other option or they accepted that the unfavourable market conditions would not allow for the offseason option to be adopted.[337]

3.57. As to the plaintiff's submission on what comprises the subject matter of a loss of hire insurance, Mance J did not accept their submission. He explained that the policy describes the interest insured as 'Loss of earnings & or expenses & or hire' and so the subject matter of the insurance is the freight or other income which the vessel could have made if it was trading.'[338] *Section 6* of the *MIA 1906* provides that insurable interest in the subject matter that is the freight and income of the vessel must have existed at the time of the loss. At the time of the accident, it was clear that the plaintiff's intention was to lay up the vessel during the off season irrespective of the damage repair therefore there was no prospect of generating an income while the vessel was in lay up so there is no insurable interest / loss of income or freight for which the insurer is expected to indemnify the assured. It is not necessary to provide evidence of the possible employment to prove loss of income however as illustrated in Capricorn the assured must show that it is their intent to place the vessel on the market and that the markets conditions are favourable enough so that there exists a reasonable possibility of employment. The assured, that is the owners or charterers of Santos must prove that they have loss income because of the spear phishing attack which has prevented the vessel from working. There is no dispute as to the intention of the parties to the charter, it was their common intention to trade and to earn an income thereby any disruption to their trade will result in loss of income. Unlike the English ABS 1.10.83 form, the Nordic Plan considers and make provision for where the vessel is wholly or partially deprived of an income, an issue dealt with at common law in the English system. If the vessel is unable to operate due to the damage, then it will be wholly deprived of income. Despite this general understanding, the

[336] Ibid.
[337] Ibid 629.
[338] *Cepheus Shipping Corporation v Guardian Royal Exchange Assurance* [1995] 1 Lloyds Rep 622, 637.

parties in their contract of affreightment may agree that 'the vessel will remain offhire until it is restored to its earlier condition'. This means that the vessel will be treated as wholly offhire even if the vessel is partially able to perform the services required of it.[339]

3.58. It is the security risks associated with the spear phishing attack which caused the owners and management of Santos to take precautionary measures in deciding to halt all operations onboard the vessel. This was believed to be the safest and most certain way of limiting further risks to the vessel and the onshore facility that was directly targeted. In responding to this incident and the delays resulting therefrom, the loss of hire insurer may need to consider several of the issues already discussed but in addition to those points consider the rules of chapter 3 of the Nordic Plan. The rules in clause 3-22 on safety regulations concerns 'measures for the prevention of loss issued by public authorities which is stipulated in the insurance contract and prescribed by the insurer pursuant to the insurance contract or issued by the classification society'[340] This definition will certainly include publications by the IMO, National Institute of Standards and Technology (NIST) and BIMCO. Classification societies such as Lloyds Register have created or forged partnerships with cyber security companies in developing a framework for threat assessments and risk management to ensure that shipowners are compliant with the said guidelines.[341] With the emphasis placed on safety within the industry, insurers are quick to include similar clauses in their policies to minimize or exclude any loss the assured may incur due to their failure to adhere to these cyber security guidelines.

---

[339] Haakon Stang Lund, 'Handbook on Loss of Hire Insurance' (Norwegian Hull Club, 3rd edn. 2016) Part 4-3-< <https://www.norclub.com/casualty-response/loss-of-hire?a=Introduction> accessed 18 September 2022.

[340] The Nordic Marine Insurance Plan 2013 version 2019, Clause 3-22. Safety regulation is a rule concerning measures for the prevention of loss, issued by public authorities, stipulated in the insurance contract, prescribed by the insurer pursuant to the insurance contract, or issued by the classification society.
Periodic surveys required by public authorities, or the classification society constitute a safety regulation under sub-clause 1. Such surveys shall be carried out before expiry of the prescribed time-limit.
When establishing the Safety Management System that is necessary to fulfil the assured's obligation to comply with the International Safety Management Code as adopted by IMO, the assured shall ensure that the system includes instructions and procedures for the use and monitoring of lubricating oil, cooling water and boiler feed water. Cl. 3-25, sub-clause 2, shall not be applied.

[341] Lloyd's Register, 'Cyber Security BIMCO Guidelines: Assessing compliance to the BIMCO guidelines' (2020) <https://www.lr.org/en/bimco-guidelines/> accessed 18 September 2022.

3.59. Clause 3-25 absolves the insurer of any liability for the breach of a safety regulation except where the loss is not a consequence of the breach, or the breach was not due to the negligence of the assured. If the breach was caused by the assured who is also the master of the vessel or a member of the crew and the breach was in connection with his employment as a seaman, the insurer may exercise his discretion not to invoke this clause and instead accept full liability for the breach. A breach of a special safety regulation that has been incorporated in the insurance contract caused by the negligence of a person whose duty it was to comply or ensure that the regulations are complied with on behalf of the assured shall be treated just the same as the negligence of the assured. The insurer has the burden to prove that there was a breach of the safety regulation whereas the assured has the reverse burden to prove that he was not negligent in the breach of the safety regulations and that there was no causal connection between the breach and the casualty. If the assured or his agent intentionally or through gross negligence breach a safety regulation of material significance, the insurer may cancel the insurance by giving 14 days' notice that only take effect upon the vessels arrival at a safe port which accords with the insurer's instructions.[342] As it relates to the scenario, while no mention is made of the incorporation of any safety regulation, the ISM code will apply by implication based on chapter IX of the Safety of Life at Sea (SOLAS), Management for the Safe Operation of Ships which makes it mandatory for the application of the ISM code to all vessels engaged in international voyages.

3.60. There is a consensus here that the cyber security breach was due to the negligence of the shipowners and that there is a causal connection between that breach / negligence and the loss of hire. It is however unclear how the insurers would respond to such a security breach, whether a spear phishing attack and social engineering breaches would amount to a breach of safety

[342] Nordic Plan 2013 version 2019 Clause 3-27 – Right of the insurer to cancel the insurance: The insurer may cancel the insurance by giving fourteen days' notice, but with effect at the earliest on arrival of the vessel at the nearest safe port, in accordance with the insurer's instructions, if:

a. the vessel, by reason of unsuitable construction, a defect, a casualty or similar circumstances, is not in compliance with a technical or operational safety regulation,

b. a safety regulation of material significance has been infringed, intentionally or through gross negligence, by the assured or by someone whose duty it is on his behalf to comply with the regulation or ensure that it is complied with.

regulations of material significance which would warrant a cancellation of the insurance under the Nordic Plan. The commentary to clause 3-27 subclause b states that the type of safety regulation will not make any difference suggesting that the insurers ability to cancel will apply both to cyber security regulations as well as the more traditional physical security regulations. Though the insurer does not need to prove his reason to cancel is justifiable or reasonable, here it is unlikely that the insurer will cancel since establishing there was intentional or gross negligence on the part of the Santos shipowners, or his employee will be difficult. Noteworthy is the acknowledgement by insurers that not all incidents of negligence or 'breach' of security regulations mentioned in the policy that will permit the cancellation of the policy. In the same way an assured is not expected to have an immaculate security management system, there will be hiccups but what is important is that the assured establishes, implements, monitors and maintain an adequate system reflective of the most current cybersecurity recommendations / requirements.

Some charterparty agreements will incorporate the BIMCO Cyber security clause 2019 or a variation of it, for that reason a brief examination of its terms is important in understanding how Santo's shipowners and its charterers will apportion liability for cybersecurity breaches that affects the operation of the charter / vessel.

BIMCO CYBER SECURITY CLAUSE 2019

In this Clause the following terms shall mean:

"Cyber Security Incident" is the loss or unauthorised destruction, alteration, disclosure of, access to, or control of a Digital Environment.
"Cyber Security" is technologies, processes, procedures and controls that are designed to protect Digital Environments from Cyber Security Incidents.

"Digital Environment" is information technology systems, operational technology systems, networks, internet-enabled applications or devices and the data contained within such systems.

(a) Each Party shall:
(i) implement appropriate Cyber Security measures and systems and otherwise use reasonable endeavours to maintain its Cyber Security;

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

(iii) regularly review its Cyber Security arrangements to verify its application in practice and

maintain and keep records evidencing the same.

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

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

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

(1) promptly take all steps reasonably necessary to mitigate and/or resolve the Cyber Security Incident; and
(2) as soon as reasonably practicable, but no later than 12 hours after the original notification, provide the other Party with details of how it may be contacted and any information it may have which may assist the other Party in mitigating and/or preventing any effects of the Cyber Security Incident.

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

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

The first disclaimer from the drafting committee about this clause is that it was not designed to address payment fraud which may be a major issue in the facts herein. The clause is definitely a step in the right direction, however does it really help a cargo owner whose goods have been damaged under a charter due to the delay caused by a cyber-attack? Does the clause place clear obligations on the parties of a charter agreement?

3.61. The word 'appropriate' is repeated throughout subclause a (i– iii) as the standard to which each party is expected to implement cybersecurity systems and plans to maintain, respond and mitigate any possible cyber-attack. In the explanatory notes to this clause, the drafters did not state the meaning to be given to 'appropriate', rather they clarified the word choice. They explained that "appropriate" is used because the level of cyber security will vary depending on several factors. It will depend on aspects such as the size of the company, the geographical location and the nature of its business. The parties are also required to maintain the cyber security measures and systems, not just implement them." What this means is instead of proposing that all systems are maintained

at desired standard across the industry, the drafters are saying "appropriate" will depend and vary based on the factual and geographical circumstances and the nature of the business which appears to be synonymous to the contractual test of reasonableness. This approach generates uncertainty and makes it more difficult to have a standardized approach in line with IMO Resolution MSC.428 (98) and one in which all parties are on an equal playing field when at risk of or during a cyber-attack. If 'appropriate' is to be so interpreted, this will be a direct analogy to the weakest link along a chain. If the charterer is the smaller business whose physical office and staff operate in a less technologically advanced and cyber secure space, 'their level of appropriateness' will be targeted by cyber criminals which will eventually expose the shipowners and other stakeholders along the supply chain at risk. If there is uniformity as it relates to the standard of cybersecurity that is to be maintained and not measured against appropriateness as described in the explanatory notes, risks will be reduced significantly.[343] There will be less unease as to whether the party with which you are contracting has maintained their cybersecurity systems to the best standards. The pooling of resources may be a viable option so that even small and medium sized businesses will have access to the highest professional and technical support for their cyber needs so there are no excuses raised based on the financial status of one party compared to the other. The purpose of a cyber security clause in a charterparty is to introduce clarity, which this clause has failed to do. The aim should be to eliminate the varying levels of cybersecurity and not to encourage a bare minimum approach among stakeholders within the shipping industry.

3.62. Subclause a (i) provides that each party has an obligation to implement appropriate systems and otherwise use reasonable endeavours to maintain its cybersecurity. Is this an option for the parties in that if they are unable to implement 'appropriate measures and systems', they would have fulfilled their obligation if they used reasonable endeavours to maintain their cybersecurity. This interpretation is unlikely the intent of the drafters as how would a party be expected to

[343] Widely used examples of these standards include ISO/IEC 27001 and ISO/IEC 27002. ISO/IEC 27009 is recommended because users will be allowed to create more sector specific standards and applications to protect and support information security, cybersecurity and privacy protection in the marine sector. Details of these standards can be accessed on the website of the International Organization for Standardization at
< https://www.iso.org/isoiec-27001-information-security.html> accessed 10 April 2022.

maintain their cybersecurity if they did not implement such systems. Furthermore, if the alternative was optional, 'or' would be substituted for 'and' between systems and otherwise. Again, the language is vague and does not provide much guidance to parties of a charter agreement in explaining to them at minimum what will be accepted as 'reasonable endeavours' or what is the standard against which 'reasonable endeavours' will be measured. However, like the explanation given for 'appropriate' and in line with its legal definition, 'reasonable endeavour' will depend on the circumstances under which each party is operating, the nature and size of the business including its geographical location. The obligation to use reasonable endeavours is extended to the third parties including brokers and agents that contract and work on behalf of the charterers and owners. Judicial decisions have reported that there is no difference between the obligation to use 'reasonable endeavours and best endeavours'.[344] In *Jet2.com Limited v Blackpool Airport Limited,* Lord Justice Moore-Bick said the natural meaning of the expression to use all reasonable endeavours is for the party under obligation do its best to ensure the obligation is met.[345] It was also agreed that the obligation to use best or reasonable endeavours shared the same meaning and did not oblige parties to act contrary to their commercial interests.[346] Furthermore, 'the obligation to use reasonable endeavours continues until the point at which all reasonable efforts have been exhausted[347].

3.63. Subclause (D) gives the parties the opportunity to decide on the liability cap. If the parties decide not to fill in the limit, the default amount of USD 100, 000 will apply. However, it is in the commercial interest of parties to always fill in the blank lines with a liability cap based on the risks and the liabilities that each party may be exposed if a breach occurs. The default amount is low compared to potential losses from a cyber incident particularly among shipping companies and their supply chains and even here where shipowners lose hire. This is the reason the drafters found it prudent to include an exception to the maximum liability stated or the default figure. These

[344] *Overseas Buyers v Granadex* [1980] 2 Lloyd's Rep 608, 613; *Rhodia International v Huntsman International* [2007] EWHC 292.

[345] [2012] EWCA Civ 417 [15].

[346] ibid para 16.

[347] [2012] EWCA Civ 417, para 26 citing Lewis J in Yewbelle Ltd v London Green Development Ltd [2006] EWHV 3166 (Ch) (unreported).

limits will not apply where the cyber-attack is the sole result of the gross negligence or wilful misconduct of a party. As concluded above and will similarly apply here, the shipowners' failure to ensure the employees were properly trained to recognize phishing emails or the systems had multiple layers of protection against phishing and malware is negligence but falls below gross negligence and was not wilful misconduct to trigger the operation of the exclusion so that whatever value is stated will be the applicable limit of liability. There is a recurrence of the theme of gross negligence, wilful misconduct or intentional behaviour which is also a criteria used in the Nordic Plan before an insurer would be permitted to cancel the policy and under the BIMCO clause as an exception to the limit identified in the clause emphasising the philosophy that not all incidents of breach of a security plan will cause the assured to lose all protection under the charterparty or from his insurers.

B. Cyber Liability Insurance: Social engineering clause

3.64. Cover for loss from a fraudulent transfer of funds can be found under the social engineering clause of many cyber insurance policies. Other insurers for example, Zurich offers this under the Crime section of their cyber policy:

> **Social Engineering**
>
> "We will indemnify you for loss resulting directly from an insured company having in good faith transferred any of your money, securities or goods in reliance upon a transfer instruction purportedly issued by an insured person, customer or vendor but which transfer instruction proves to have been fraudulently issued by an imposter without the knowledge or consent of the insured person, customer or vendor provided that such loss is first discovered and is notified to us during the period of insurance.
>
> Excluding the first £5000 of any loss."[348]

For most social engineering clauses, the only loss that will be indemnified by insurers are those direct losses resulting from the fraudulent transfer instructions. Consequential losses will not be covered neither will losses to dependent third parties who have suffered loss because of the social engineering attack. This means as assureds of this policy, the shipowners of Santos would only be

[348] Zurich Insurance plc, 'Cyber Policy Section B- Crime: Social Engineering ' SME513C.04 (NP721418004) (10/20) CMS <https://www.zurich.co.uk/business/business-insurance/specialty-lines/financial-lines/cyber> accessed 18 September 2022.

able to recover the hire earned that was transferred to the cyber criminals in good faith and without knowledge or consent of the assured, customer or vendor and the insurer must be notified of the transaction during the period of the policy. Unlike some of the 'direct loss' cases and 'unauthorised access' cases discussed, there is no issue as to the assured, customer or vendor being involved in the transaction by receiving and sending the instructions to the hackers provided they acted in 'good faith', without fraudulent or malicious intent. Therefore, the employee's action would not break the chain of causation so that the insurer would be absolved from indemnifying the assured the hire transferred to the hackers. Aviva Insurance will reimburse the assured for the cyber extortion monies paid and the costs necessarily and reasonably incurred to resolve the cyber extortion provided it is legal to do so however they will not cover for more than 1 claim arising from the same extortionist.[349]

3.65. Assureds must be keen to abide by the conditions stated in their policy before a cyber extortion payment will be reimbursed. Failure to meet the following conditions will cause the insurers not to pay the claim. Aviva Insurers for example, expect the assured upon receiving a cyber extortion demand to immediately notify the insurers and comply with the requirements of the claims service provider and for UK businesses to immediately notify Action Fraud of the Cyber Extortion. Additionally, the assured should take all steps to mitigate the loss and should not disclose the existence of cyber extortion cover except where such disclosure is required by law to the relevant law enforcement authorities. The reasoning behind nondisclosure of the existence of cyber endorsement cover is that cybercriminal and even insiders may be encouraged to target the assured as the likelihood of their request being met increases if there is insurance for such loss.

III. Chapter Summary

- The spear phishing attack can cause a vessel to be offhire if the security breaches resulted in the loss of time and has hindered or prevented the full working of the vessel and it is not in an efficient state to perform the services required of it.

[349] Aviva Insurance Ltd, 'Cyber Insurance Policy Section : Extortion' (BCOAG15081 12.2020) <https://www.aviva.co.uk/adviser/documents/view/bcoag15081.pdf> accessed 18 September 2022.

- An offhire clause with the words ‘efficient state of the vessel’ applies a more restrictive meaning in that the event or cause of the loss must be internal to the vessel itself, thus where those words are present in the offhire clause within a charter party agreement, it is unlikely that a vessel will be offhire based on a cyber-attack caused by a malicious third party.

- A cyber-attack will not be classified as an offhire event based on the qualification ‘deficiency and or default and or strike of officers or crew’ under clause 17 line 220 of the NYPE form as ‘default’ does not include negligence. This is correct even if the security breach was due to the negligence or failure on the part of the management team to adhere to BIMCO and other industry guidelines encouraging assureds to identify as vulnerabilities ‘shipboard computer networks which lack boundary protection measures and segmentation of networks’.

- A spear phishing attack and by extension a cyber-attack will not qualify as one of the named offhire events or fall into the category of ‘any other cause preventing the full working of the vessel’ since it is unlikely that a spear phishing attack will be related to the physical condition or efficiency of the vessel. However, a cyber-attack may qualify under the wider ‘any other cause whatsoever’ as the event need not be related to the physical condition or efficiency of the vessel or crew. To remove the uncertainties and the questions about whether specific cyber event fits into the offhire hire clause, it is prudent to add cyber-attacks or computer related breaches to the list of offhire events.

- A spear phishing attack may qualify as an offhire event even in circumstances where the vessel is not completely dysfunctional, for example where there has been a partial malfunction or reduction in services such as the speed and manner in which a service is usually done is negatively affected.

- Where a charterer delays or fail to pay hire as a result of a cyber-attack, the shipowner retains the right to suspend the performance of any or all obligations under the charterparty agreement but throughout the period of suspended performance, the vessel remains on hire provided cyber risk is not among the perils named in the offhire clause.

- The BIMCO Non-Payment of Hire Clause for Time Charter Parties 2006 is limited in its application to cyber risks as it does not consider situations where payment is fraudulently diverted or even where a notice is served for the hire to be paid within 72 hours, the difficulty or impossibility of charterers meeting that obligation when either or both the charterers and the shipowners' systems have been hacked.

- A claim for loss of hire under clause 1(a) of The standard Loss of Charter Hire Insurance Including War (ABS 1/10/83) and Loss of Charter Hire Insurance Excluding War (ABS 1/10/83) is closely interconnected with a claim in consequence of loss, damage or occurrence covered Institute Time Clauses-Hulls (1/10/83) and also loss damage or occurrence covered by Institute War and Strikes Clauses-Hulls (1/10/83). Therefore, a cyber-attack which resulted in loss of hire without physical damage or loss would not be covered under the ABS 1/10/83 without modification to include an endorsement clause on cyber risks.

- There is another school thought that revived after the Court of Appeal decision in (The "Wondrous") [1992] 2 Lloyds Rep 566 where the court was asked to determine whether there is a requirement for the vessel to be physically damaged before a loss of hire insurer will be engaged in the conversation as to liabilities. The CA decided that loss or damage to the vessel is germane to a loss of hire policy, however if parties so intend, they may give the loss of hire policy wider meaning than the hull policy so that loss of hire will be recoverable irrespective of loss or damage to the vessel.

- The BIMCO Cyber security Clause 2019 is a step in the right direction but falls short in that it failed to clearly describe the standard to which each party is expected to implement cybersecurity systems and plans to maintain, respond and mitigate any possible cyber-attack but rather simply stating that cybersecurity measures and plans should be 'appropriate'. The explanation is that appropriate is used because the level of security will vary depending on various factors such as the size of the company, the geographical location and the nature of the business. Essentially leaving cyber criminals to prey on the weakest link in the supply chain.

This approach generates uncertainty and makes it difficult to have a standardized system in line with IMO Resolutions MSC.428 (98) and one in which all parties are on equal standing when at risk of or during a cyber-attack.

- Maintenance of a uniformed minimum standard and not a system modelled on appropriateness as described in the explanatory notes to the clause will significantly reduce targeted attacks on for example small and medium sized businesses along the supply chain. The pooling of resources may be a viable option so that small and medium sized businesses will have access to the highest professional and technical support to implement, maintain and monitor their cyber security needs.

- Charterers and shipowners may be able to recover hire or monies loss from their cyber insurance insurer as a direct result of fraudsters impersonating company employees, customers or vendors through a social engineering attack from their cyber insurance insurer provided the transfer was made in good faith, without the knowledge or consent of the assured, the customer or vendor.

Scenario 3: Onboard Data Breach

Time to relax and enjoy some entertainment onboard!

Alvin, a crew member onboard Santa Maria, a passenger vessel owned by Caribbean Cruise Line connected his cell phone to the ship's internet network. Alvin innocently accessed the internet to stream a music video and visit his social media websites but unknown to him, the link selected has a malware (virus) which corrupts and destroys all the data stored on the ship's system. Consequently, personal and company data was stolen, and software was damaged, the impact of which was aggravated because the vessel intranet was directly connected to its parent company onshore.

Content **Pages**

I. Onboard Data Breach

Privacy lies at the heart of liberty in a modern state. A proper degree of liberty is essential for the well-being and development of an individual.[350]

A. Data Breach and **Privacy rights**

4.1. The right to privacy and the right to data protection are interconnected yet they are treated differently by international conventions and domestic laws within the UK. The right to privacy has been protected by *Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)* where it is listed as a fundamental human right. While the right to protection of personal data is covered by the Data Protection Act 2018. The right to data protection is a more modern right that has developed mainly due to the increased breaches in information and operational technology, it is a right that can be categorized as a subset of the fundamental human right to privacy, therefore such arguments will begin to circulate and take prominence more than they have before. Privacy rights are encroached upon and are more frequently and blatantly violated each day as cyber-attacks proliferate, which means that few minutes of 'fun online' could cause billions in losses, some irrecoverable and others irreplaceable and a lifetime lesson. Alvin, a crew member onboard Santa Maria was excited about his lunch break to have some well-deserved 'fun' online, little did he know that his few minutes of entertainment on a personal device could have led to the extensive losses incurred in this scenario. The series of events occurred after Alvin connected his cell phone to the vessels internet and having done that, he unintentionally introduced a malware to the company's internal storage system which infiltrated and corrupted both personal and company data. The consequence of the malware led to data being corrupted and stolen by the unidentified third parties responsible for creating the malware. While the incident may surprise Alvin, it is common knowledge that there is no uncertainty about the occurrence of cyber-attacks, any doubt will relate only to their timing. Accordingly, Alvin along with his employers should be aware of the vulnerabilities to systems connected to the internet. In fact, the information age and the internet of things provide the platform

[350] *Campbell v. MGN Ltd* [2004] 2 AC 457 [12] (Lord Nicholls).

and germination site for these types of incidents. To put things into perspective, the objective of this chapter is to define what has happened in the scenario, discuss the losses, liabilities and the insurance implications that will arise from the incident onboard Santa Maria. Finally, there will be a discussion as to whether the traditional marine insurance and the newer data liability policies are adequate to protect the assured against the losses and liabilities arising from the data breach.

4.2. The incident will be classified as a data breach as defined in *section 33 of the Data Protection Act 2018 (DPA 2018)*. A personal data breach means 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed'.[351] The definition focuses on personal data breach as the regulations and laws addressing data protection are primarily concerned with the data of the identified or identifiable living individual[352] and not that of the artificial person ascribed to companies by the *Companies Act 2006*[353]. This definition befits the scenario since there has been the loss and corruption of personal data more specifically data belonging to the crew, other employees and possibly the past and current passengers of Santa Maria. An identified or identifiable living individual, can be identified either by reference to a unique identifier such as their name, identification number, location number or online identifier'[354] or 'one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.'[355] Those are the biographic data which a passenger vessel will have stored about its passengers and crew members thus there is great potential for data protection laws and regulations to be breached.

4.3. A data breach may initially seem far-fetched and unrelated to the shipping industry, however as discussed in scenario 2, cyber-attacks including data breaches have no prejudices and ignores all political distinctions, geographical borders and industry type. Therefore, the shipping industry is not immune to cyber-attacks or any form of internet related breaches. Recently, there has been a rise in the reporting of cyber incidents within the maritime industry partially due to the

[351] Data Protection Act 2018, Section 33 (3).
[352] Ibid.
[353] *Salomon v A Salomon & Co Ltd* [1896] UKHL 1, [1897] AC 22.
[354] Data Protection Act 2018, s. 3 (3) (a).
[355] Ibid, s.3 (3) (b).

new *General Data Protection Regulation 2018* and the lessons from cyber incidents both within and outside the industry. The sector is particularly vulnerable due to its growing reliance on information technology and the expansive supply chains that depend on its operation. Additionally, the fact that over 90% of trade in the UK is carried by sea means that the safe and continuous operation of the sector is critical to economic stability, therefore a successful cyber-attack penetrating any facility within the sector may have devastating results even if Santa Maria was the only target. Furthermore, the maritime industry is a lucrative target for cyber criminals who are interested in carrying out a data breach because of the financial background of many of the individuals who are associated with the sector and who can afford to vacation on luxury vessels and yachts. Another contributing factor to this vulnerability is the limited extent to which the staff and crew within the maritime sector are trained to identify and deal with cyber risks. A survey conducted by Futurenautics with the assistance of 6000 crew members found that only 900 which represents a minimal 15% of the seafarers had received any form of cybersecurity training.[356] Although 6000 seafarers is a small cross section of the thousands employed worldwide, the report illustrates the general concern of the lack of adequate training of most seafarers which like this scenario, is often the basis for multiplying cyber-attacks on vessels and other facilities within the industry. The results from the survey highlights some of the areas of concern, for example only 33% of the 6000 seafarers stated that their last company had a system where passwords are regularly updated and even a smaller group of 18% said their previous company had a policy requiring all default passwords to be changed.[357] These shortcomings by shipping companies coupled with untrained staff raises the risk of a data breach.

4.4. There have been many data breaches in the UK affecting companies of varying sizes and across several industry types including transport, some of these incidents will be discussed below as case studies. The relevance here is that lessons must be learnt from each incident despite the difference in industry. Many data breaches are the consequence of negligence or complete omission by management to ensure that systems are sufficiently protected, and that staff is properly

[356] Futurenautics, 'Crew Connectivity 2018 Survey Report' (2018) <https://www.futurenautics.com/product/2018-crew-connectivity-survey-report/> accessed 18 September 2022.
[357] Ibid.

trained on cyber security vulnerabilities. Those were the same ills which manifested in the scenario with Alvin and the management of Santa Maria that contributed to the chaotic state of things and the losses incurred following the data breach onboard Santa Maria. The causal dynamics of the foregoing will be discussed in the subheading which follows.

B. What's the cause, the losses and who will take the blame?

4.5. The legal principles relating to causation have already been discussed in the previous chapters so there is no need to repeat that discussion here. The proximate cause of the loss is the data breach caused by the introduction of a virus to the internal system attributable to the partial negligence and omission of the management and crew of Santa Maria. The impact of the data breach is significant. They include theft and corruption of personal and company data, software damage, financial loss, possible fines under the UK *GDPR*[358] */ DPA 2018*, legal and public relation fees, reputational damage which eventually leads to reduction in customer trust and possible loss of potential customers[359].

a. Breach Notification: CCL

4.6. The *DPA 2018* requires the data controller,[360] in this case *Caribbean Cruise Line (CCL)* to communicate without undue delay any personal breach to the data subjects that is likely to result in a high risk to the rights and freedoms of individuals.[361] Since this obligation is placed on the

[358] The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, s. 2 "the UK GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018."

[359] Alex Cravero and Peter Dalton, 'Digital Assets Theft: cybersecurity' C.T.L.R. 2016, 22 (3), 67-75. A discussion on reputational damage and loss of business opportunity is discussed in scenario 4.

[360] Data Protection Act 2018, s. 32 'controller' means the competent authority which, alone or jointly with others determines the purposes and means of the processing of personal data or s. 6 (2) 'where the personal data is processed only for the purposes for which it is required by an enactment to be processed and by means which it is required by an enactment to be processed, the person on whom the obligation to process the data is imposed by the enactment (or, if different, one of the enactment) is the controller.'

[361] The notification requirements in s.68 (1) do not apply where; i. the controller applied appropriate technological or organisational protection measures to the personal data affected by the breach, for example encryption of such data (ss. 68(3) (a) and 68(4)); ii. Where the controller has taken measures after the breach to ensure that the risk to the rights and freedoms of data subjects is no longer likely to materialise (s. 68(3)(b); iii. It would involve a

controller by virtue of *s. 68(1)* of the *DPA 2018*, it is comprehensible why CCL would be expected to cover the notification costs to inform the data subjects of the breach. Considering that Santa Maria was a passenger vessel that can accommodate thousands of passengers and crew on any one trip, it is expected that notification costs will be expensive[362] especially because multiple means of communication will need to be utilized to effectively reach passengers who may be living in various parts of the world. In addition to informing data subjects, CCL is legally expected to notify the ICO[363] of any personal breach to data subjects to which they become aware without undue delay and where feasible, not later than 72 hours after becoming aware of the breach.[364] The category of people whose knowledge will become the knowledge of the CCL will extend beyond senior management to include the chief information officer, Information and operational technology staff and data security personnel as well as other members of the organization who work closely with data handling and security. The proviso to this subsection is that there is no obligation on the part of the controller to notify the Commissioner if the personal breach is 'unlikely' to result in a risk to the rights and freedoms of individuals.[365]

i. Burden of proof and the meaning of unlikely

4.7. The use of the word 'unlikely' means that there is an even greater probability that there will be no risks to the rights and freedoms of individuals than there is an actual risk of harm.[366] The burden of proof will be on the CCL as the controller of the data to establish that harm to individuals from the breach is unlikely, however this will not be based on their assessment of the situation but based upon the viewpoint of a reasonable man.[367] The threshold is lower than if the

disproportionate effort. If the case does not fall in i or ii, the information that would be included in the notice of a breach to the data subjects must be made available in an equally effective way for example by public communication (ss. 68(3)(c) and 68(5).

[362] The average total costs for the notification aspect of data breaches in 2021 was measured as $0.27 million which accounted for 6% of the average total costs of a data breach ($4.24m global average).
IBM Security, 'Cost of a Data Breach Report 2021' (IBM Security and Ponemon Institute, July 2021), 16 <https://www.ibm.com/security/data-breach> accessed 18 September 2022.

[363] Information Commissioner's Office is the regulatory body with oversight over Data Protection in the United Kingdom.

[364] DPA 2018, s. 67 (1).

[365] Ibid, s. 67 (2).

[366] *Polurrian Steamship Co Ltd v Young* [1915] 1 KB 922, CA.

[367] *Marstrand Fishing Co Ltd v Beer* [1937] 1 All ER 158, 164.

section required the controller to prove that there would be 'no harm' from the breach. This would be an absolute, akin to 'beyond a reasonable doubt' threshold in criminal law. Similarly, there is a distinction between harm being uncertain and the unlikelihood of harm. *Wright LJ* in *Rickards v Forestal Land, Timber and Railways Co*[368] explained that when 'uncertain' is used, the balance is even, so no one can say one way or the other while unlikelihood indicates some balance against the event.' Any degree of unlikelihood would suffice despite how minute, there is no need for a major shift of the balance.

4.8. The Australian case of *TAL Life Ltd v Shuetrim; Metlife Ltd v Shuetrim*[369] departed from the mathematical test of less than 50% probability and adopted the 'no real chance' test. The main distinction according to the court in *TAL Life Ltd* is between 'possibilities which are readily contemplatable even though they may not be more probable than not and possibilities which are remote or speculative.' There cannot be a real chance of harm if the possibilities are very remote or speculative which must be assessed on the individual facts of each case. The decision will have only a persuasive effect on the courts of England and Wales and it is yet to be seen if the judges will apply the no real chance test and depend less on an attempt to read the scales of probability which is sometimes very difficult. The researcher is of the view that the 'no real chance' test will be more effective with cyber related incidents as any test based upon results from a mathematical approach will be skewed since there is limited data or models from which these trends can be properly analysed. Moreover, the reluctance or altogether refusal to report cyber incidents particularly within the maritime industry does not assist with this analysis or allow for a reasoned prediction of the likelihood of a cyber risk.

b. Loss of personal data: Emotional distress and Personal Injury

4.9. Loss of personal data after the cyber-incident onboard Santa Maria has been confirmed. The challenge for many of the data subjects is deciding the most appropriate route to successfully claim for damages against the carriers. Lodging a complaint to the Information Commissioner against a controller or processor for personal data infringements is straightforward and set out in

[368] [1941] 3 All ER 62 (HL) 81.
[369] [2016] NSWCA 68.

section 165 of the DPA 2018 and Articles 57(1)(f) and (2) and 77 of the UK GDPR. In these same pieces of legislation, the data subject is given the option to claim compensation through the court[370] without prejudice to the administrative or non-judicial process before the ICO. In this section, we will explore the possible claims in the tort of misuse of private information, breach under the relevant data protection legislation as well as the options under the Athens Convention 2002.

4.10. A claim in tort against the carriers for misuse of private information is possible. This is confirmed in *Vidal- Hall and others v Google Inc*[371] where misuse of private information was categorized as a tort. In answering the question whether compensation is recoverable for distress without financial loss the court decided that reference to 'damage' in *section 13* of the *DPA 1998* include both pecuniary and non-pecuniary damages such as distress.[372] Since the purpose of the Act was to protect data privacy rather than economic rights, it would be odd if there was no compensation to the data subject for privacy breaches devoid of pecuniary loss.[373] In fact, the main form of damage under the Act is the distress due to privacy invasion or breaches, therefore an effective remedy should be available to data subjects. Besides, a more restrictive interpretation would be inconsistent with the remedy available under the *European Convention for the Protection of Human Rights and Fundamental Freedoms (Convention)* and the objective of the Data Protection Directive to protect the fundamental rights and freedoms of individuals including the protection of the privacy rights (*Article 8* of the *Convention)* which has always permitted a remedy against non-pecuniary damage.[374] Additionally, *Article 8 of the Charter of Fundamental Rights of the EU* protects personal data therefore if a data controller would be found liable only where there has been pecuniary losses to the data subject, such interpretation would defeat the general purpose and object of conferring such status to data protection under the Charter. On a similar note, *Article*

[370] Articles 78 and 79: Right to an effective judicial remedy against the Commissioner and a controller or processor.
[371] [2015] EWCA Civ 311; [2016] QB 1003; [2016] 2 All ER 337; Aven and others v Orbis Business Intelligence Ltd [2020] EWHC 1812 (QB).
[372] *Vidal – Hall and others v Google Inc* [2016] 2 All ER 337, per Lord Dyson MR and Sharp LJ), para 76; This reproduced in Article 82(1) of the UK GDPR 2018. The word 'damage' as used in the 1998 Act does not extend to distress. It concerns only material damage. The court in *Vidal v Google* confirmed this interpretation and was able to extend the meaning of 'damage' to distress without material damage by disapplying *s. 13(2) of the DPA 1998* as being incompatible with EU law. Section (1) of the Data Protection Act 2018 has removed the ambiguity by clearing stating that 'non-material damage' includes distress.
[373] *Vidal – Hall and others v Google Inc* [2016] 2 All ER 337, per Lord Dyson MR and Sharp LJ), para 77.
[374] *Vidal – Hall and others v Google Inc* [2016] 2 All ER 337, per Lord Dyson MR and Sharp LJ), para 77.

47 of the *EU Charter* asserts that everyone whose rights have been violated must have to their avail an effective remedy. Denying the data subjects compensation because there was no associated pecuniary loss would not be an effective remedy.

4.11. In *TLT and Others v The Secretary of State for the Home Department and Another***,**[375] the claimants' personal data were exposed on an internet website operated by the Home Office. The data included information regarding the asylum proceedings of each data subject and contained their full names and the status of their case. The website was accessed multiple times by individuals who are not associated with the department and as far away as one person in Somalia. The Home Office admitted the data breach and notified the data subjects few weeks after the breach was identified but the letter which accompanied the notice did not give all the details nor did it include the heading of the spreadsheet thus the claimants could not initially get a clear idea of the seriousness of the breach. The Defendants 'admitted that the information contained in the spreadsheet amounted to a misuse of their private and confidential information, and to processing their personal data in breach of the first, second and seventh principles set out in *schedule 1* to the *Data Protection Act 1998*.'[376]

4.12. In cases of this kind where private information has been exposed, damages are an award to compensate for the loss or diminution of a right to control formerly private information and for the distress that the [claimants] could justifiably have felt because their private information had been exploited and are assessed by reference to that loss.[377] In *TLT and others*, the claimants' genuinely feared that the information exposed on the website was viewed by the Iranian authorities. They were terrified of the impact of such knowledge especially with the possibility of their return to Iran. They also gave information that members of their family in Iran were detained and questioned about them and they were concerned about the wellbeing of their teenage son and other family members in Iran. As a result of the breach and for security reasons, the family was forced to relocate which further disrupted their life and caused great distress to the family especially before they were granted asylum. The judge in assessing each claim likened the issues

[375] [2016] EWHC 2217 (QB).
[376] ibid 10.
[377] ibid 18.

to awards made in psychiatric injury cases and considered all the factors as a result of the breach which could have affected the mental state or caused some degree of shock to the victim and whether their state of being described was a rational consequence of the breach. In the case of PNA who was one of the claimants, the court rejected her claim as it was not rational to believe from the breach, her husband's family in Pakistan would be able to locate her. It is irrational because the information published did not include information which the family did not already know, and her full address was not disclosed on the website. As a result, PNA could not be compensated for distress due to her reliance on these facts, instead she will only be compensated for the immediate shock caused by the posting of the information and the possible consequences. While it is conceded that the passenger information held by Santa Maria's company will not be as sensitive nor will it usually be used for direct physical or violent threats such as those experienced by asylum seekers in TLT, nonetheless the passengers credit card information inclusive of the passengers' full name, date of birth and address are all very lucrative and sensitive data for financial and identification crimes online. As is evident from the cases, acceptance of a claim for distress due to a data breach without pecuniary loss will depend on the sensitivity of the information and the purpose for which the data will be used.

4.13. Another case discussing *s. 13* of the *DPA 1998* is *Lloyd v Google LLC*[378]. The claimant Mr Lloyd who represented over 4000 iPhone users allege that Google tracked their internet activity and sold their personal information for commercial purposes. The facts are similar to *Vidal- Hall* but the distinguishing feature is that in *Vidal-Hall*, the claimants seek individual damages based on the distress they experienced whereas in *Lloyds v Google LLC*, a collective claim was made on the basis that the claimants' information was used without their permission. Mr Lloyd's case is that compensation is recoverable under *s.13(1) of the DPA* 1998 without proof of material damage or distress when a data controller contravenes any requirement of the Act relating to the personal data of data subject / victim of the breach. The loss or contravention must not be trivial or de minimis. Mr Lloyd's claim was rejected, it was decided that *s.13 of the DPA 1998* does not give a data subject the right to compensation for any non-trivial

[378] *[2021] UKSC 50.*

contravention of the Act without proof of material damage or distress arising from such contravention.[379] Without evidence of damage from each member of the represented class, it is impossible to meet the required threshold for an award of damages.[380] The mere fact there has been widespread infringement of privacy rights does not mean a representative claim will be successful. If the representative procedure is selected, the Claimants must produce evidence to establish damage to each individual member of the class caused by the contravention of the Act. Each member would also need to establish the extent of unlawful processing in their individual case.

4.14. Lord Legatt in his judgment in *Lloyds v Google LLC* referred to *Gulati v MGN Ltd*[381] where the Court of Appeal discussed damages that is to be applied for wrongful invasion of privacy. The facts concerned the test case of eight (8) famous claimants whose phones were hacked by newspapers leading in some instances to the publication of articles on information retrieved from the devices. The Defendants admitted liability for the breach but argued that in absence of material damage, the only compensation allowed was for distress caused by the breach of privacy. *Mann J* disagreed, he decided that 'there is no principle why an award for damages for distress could be allowed but no award for the infringement of the right in itself'.[382] The Court of Appeal agreed and held that '… the power of the court to grant general damages was not limited to distress and could be exercised to compensate claimant also for the misuse of their private information'.[383] The Court of Appeal also rejected the submission that the grant of an award of damages for intrusion of privacy without associated distress is inconsistent with the principle that vindicatory damages are not an available remedy for violation of a private right. *Arden LJ* held there was no question relating to the award of vindicatory damages and that the purpose of the awards was 'to compensate for the loss or diminution of a right to control formerly private information'.[384] Based on *Vidal* and *Gulati*, Mr Lloyd would have the following

[379] *[2021] UKSC 50,* para 138.
[380] *[2021] UKSC 50,* para 153.
[381] [2015] EWHC 1482 (Ch); [2016] FSR 12 and [2015] EWCA Civ 1291; [2017] QB 149.
[382] Para 100, citing Mann J in [2015] EWHC 1482 (Ch); [2016] FSR 12, para 11.
[383] Para 102, citing Arden LJ in [2015] EWCA Civ 1291; [2017] QB 149, para 45.
[384] *[2021] UKSC 50,* para 103.

two options: to claim damages under *s. 13 (1) of the DPA 1998* for distress suffered as a result of Google's contravention of any requirement of the Act and or damages for the misuse of private information without the need to prove that it caused material damage or distress.

4.15. Lord Legatt did not agree that the claim can be made without material damage because the *DPA* and *the Data Protection Directive (DPD) 1995* share a common source, in protecting privacy rights of an individual. Moreover, the claimants' reliance on the decision in *Gulati did not* advance their claim. In fact, he found no reason why the basis on which damages are awarded for a domestic tort should be relevant for the interpretation of the term damage in a statutory provision intended to implement a European Directive.[385] The fact that both have their foundation in protection of personal privacy specifically *Art 8* of the *Convention* is also not reason for transfer of principles regarding the award of damages.[386] There are many differences between data protection legislation and common law tort of misuse of information as such it cannot be accepted that decision in *Gulati* is applicable by analogy to the *DPA 1998*. The first difference is that the DPD 1995 and the DPA 1998 apply to all personal data with no requirement that it is of a confidential or private nature or there exist a reasonable expectation of privacy. On the other hand, the common law tort of misuse of information requires that there is a reasonable expectation of privacy. The second difference is that under the DPA 1998, the data controller must have failed to exercise reasonable care in order for the claimant to be entitled to compensation.[387] For the regular consumer / data subject, it is recommended that claims for breach of privacy rights are made both under the common law tort of misuse of private information and under the relevant data protection legislation.

4.16. Whether damages for distress caused from the loss of the personal data of passengers will be recoverable under the compensation regime of the *Athens Convention* has not been examined in any case law. That decision would depend on whether a data breach or cyber-attack which causes personal injury will qualify as a shipping incident as defined under the Athens Convention

[385] Para 124.
[386] Para 129.
[387] Para 132.

2002. However, the judicial precedent to date has indicated a trajectory where many of these cases have been settled in tort law, outside the realm of the Athens Convention for the obvious reason that the cases did not involve data breach onboard a passenger vessel. Based on the discussion above, the passengers will also be able to pursue their claim in tort for misuse of private information and or under the Data Protection Act 2018. Aside from those two options, the analysis immediately below will look at potential passenger claims under the Athens Convention against the carrier / shipowners as controllers of their personal data with the prospect of recognizing the mental distress arising from a data breach as a type of personal injury and a basis on which claims can be successfully made.

C. Attribution of Liability

a. CCL as the Carrier: Athens Convention 1974 and 2002 Protocol

4.17. *The 1974 Athens Convention* relating to the carriage of passengers by sea and their luggage is incorporated in the United Kingdom by virtue of *s. 183 of the Merchant Shipping Act 1995*. The terms of the Convention found in *Schedule 6 of the MSA 1995* applies to any contract of carriage of passengers by sea both within domestic and across international waters[388]. *Article 1(a)* and *(b)* define carrier as 'a person by or on behalf of whom a contract of carriage has been concluded' while the 'performing carrier means a person other than the carrier, being the owner, charterer or operator' of the vessel. It is a requirement that the carrier give notice to the passengers that the Convention shall apply to their contracts of the carriage, the terms of which are usually on the back of their tickets. Failure to bring the application of the Convention to the attention of the passenger could make the carrier liable on summary conviction to a fine.[389] In most instances of death, personal injury, loss or damage to luggage, the claimant has the burden to prove that there was fault or neglect on the part of the carrier. Provided that the claimant has discharged his burden, the carrier shall be liable for death, personal injury or damage which occurred during the carriage[390].

[388] The Carriage of Passengers and their Luggage by Sea (Domestic Carriage) Order, 1987.
[389] S.I. 1987/703.
[390] 1974 Athens Convention, Article 3.

There are few exceptions to this general rule which have been expressly stated in *Articles 3* and *4* of the *Convention* as amended by the Protocol of 2002.

b. Is the data breach a shipping incident?

4.18. A shipping incident as defined in the Athens Convention means shipwreck, capsizing, collision or stranding of the vessel, explosion or fire in the ship, or defect in the ship. [391] The carrier will only be liable for loss which arises from incidents that occurred in the course of the carriage, a fact which the claimant would need to establish.[392] Both the carrier and the performing carrier will be held jointly and severally liable for the performing carrier's section of the carriage; these liabilities will extend to the acts and omissions of their servants and agents[393]. If the *Athens Conventions* should be applied to the facts of this scenario, a genuine concern is whether the data breach can be treated as a shipping incident? The answer to this question is important as the liability regime under the Convention varies depending on whether the passenger's death or personal injury is caused by a shipping (strict liability) or non-shipping incident (fault-based liability). For loss caused by death or personal injury due to a shipping incident, the carrier will be strictly liable up to 2500, 000 units of account[394] for each distinct occasion of loss to each passenger unless the carrier proves that the incident resulted from an act of war or other hostilities or a natural phenomenon of exceptional, inevitable and irresistible character; or was wholly caused by an act or omission done with the intent to cause the incident by a third party. If the loss exceeds

[391] Articles 3 and 3 (5)(a), Merchant Shipping (Convention Relating to the Carriage of Passengers and their Luggage by Sea) Order 2014 (SI 2014/1361) Schedule New Part I to be Substituted in Schedule 6 to the Act; Article 3 (5) of the Protocol of 2002 to the Athens Convention relating to the Carriage of Passengers and their Luggage by Sea, 1974.
[392] Article 3(6) Protocol to Athens Convention 2002.
[393] Article 4 (1)-(2) and 4(4) Athens Convention 1974.
[394] Unit of accounts as defined under Article 9 of the Convention is the Special Drawing Right as defined by the International Monetary Fund. The amounts mentioned in Article 3, paragraph 1, Article 4bis (1), Article 7 (I), and Article 8 shall be converted into the national currency of the State of the court seized of the case on the basis of the value of that currency by reference to the Special Drawing Right on the date of the judgment or the date agreed upon by the parties. The value of the national currency, in terms of the Special Drawing Right, of a State Party which is a member of the International Monetary Fund, shall be calculated in accordance with the method of valuation applied by the International Monetary Fund in effect on the date in question for its operations and transactions. The value of the national currency, in terms of the Special Drawing Right, of a State Party which is not a member of the International Monetary Fund, shall be calculated in a manner determined by that State Party.

250,000 the carrier shall further be liable up to 400,000 SDR[395] unless he proves that the incident which caused the loss occurred without the fault or neglect of the carrier.[396] As it relates to loss as a result of death or personal injury to a passenger caused by a non-shipping incident, the carrier will be liable if the claimant can prove that the incident which caused the loss was due to the fault or neglect of the carrier.[397]

4.19. *Article 3(5) of the Protocol to the Athens Convention 2002* cites stranding, collision, grounding inter alia which are common marine incidents, but could a cyber-attack of this nature be classified as a marine incident analogous to the ones mentioned above? A cyber- attack specifically a data breach is not the type of incident that the drafters of the Convention contemplated, however that cannot be the only basis on which a decision is made as to the suitability of the application of the Convention to this incident. If the sui generis rule is to be applied, the examples of risks that qualify as a shipping incident is of a different nature than a cyber-attack. The risks listed as a shipping incident are directly related to the physical vessel interacting with the sea resulting in an incident that is somewhat unique to vessels or other facilities operating at sea. On this basis, the cyber-attack specifically the data breach cannot be considered a shipping incident synonymous with those named in the Athens *Convention.* Accordingly, the strict liability regime of the Convention would not apply to the facts, thus the burden will be on the claimants to establish on a balance of probabilities that CCL should be held responsible for the losses arising from the data breach. The claimants will need to prove that the injury, loss or damage occurred during the course of the voyage, the extent of the loss or damage, [398] it was due to the fault of the carrier, or his servants or agents and that the latter was acting within the scope of his employment.[399]

4.20. Notwithstanding the futility or success of those points, the most convincing argument will be that the data breach arises from a defect in the ship. Unlike the collision, stranding and the perils

[395] Protocol to Athens Convention 2002, Article 7
[396] Ibid Article 3 (1).
[397] Ibid Article 3(2).
[398] Ibid Article 3(6).
[399] Protocol to Athens Convention 2002, Article 3(5)(c).

named, defect in the ship is not limited to damage to the physical hull of the vessel. Article 3(5)(c) defines defect in the ship as any malfunction, failure or non-compliance with applicable safety regulations in respect of any part of the ship or its equipment… or when used for the propulsion, steering, safe navigation, mooring, anchoring, arriving at or leaving berth or anchorage…[400] Generally, such wide definition of the defect in the ship will unquestionably include cyber-attacks caused by failure or non-compliance with safety regulations, any part of ship or its equipment when used for specific purposes. The latter part of definition restricts the application so that not every incident involving the malfunction or non-compliance with a safety regulation will qualify as a shipping incident to trigger the strict liability regime of Article 3(1) and enable direct claims against the liability insurers. Therefore, it is important to think about the nature of the breach and whether it has affected the navigation instruments such as the GPS, AIS, bridge controls or other parts of the vessel used for disembarkation, anchoring, mooring, or arriving at and leaving berth.[401] So while the cyber-attack in chapter 1 on piracy which affected the navigation instruments may qualify as a defect in the ship, another cyber-attack such the data breach onboard Santa Maria may not qualify as a defect in the ship because it has not affected the navigation or embarkation /disembarkation or berthing facilities of the vessel. However, if the cyber-attack resulted not only in personal data theft but also affected the safety, navigation or evacuation facilities of the vessel, there is no reason why the cyber-attack could not be classified as a shipping incident and defect in the ship. If as is argued here, the data breach onboard only affected the personal data of the crew and passengers, it is unlikely to qualify as a defect in the ship or a shipping incident.

4.21. Moreover, the fact that a cyber-attack may endanger the safety of the vessel and those onboard should qualify the risk as a shipping incident enough to trigger the strict liability regime in the Athens Convention. Furthermore, as the industry becomes more autonomous, the threats to shipping and the events traditionally identified as examples of shipping incidents will morph into more digitized versions and to include incidents such the data breach onboard Santa Maria and

[400] Protocol to Athens Convention, Article 3(5)(c).

[401] George Leloudas, 'Cyber Risk, Autonomous Operations and Risk Perceptions: Is a New Liability Paradigm Required?' p. 108-109 in Baris Soyer and Andrew Tettenborn (editors) *Artificial Intelligence and Autonomous Shipping: Developing the International Legal Framework* (Hart Publishing 2021).

other cyber-attacks. The overriding objective of the Athens Convention is to protect the passengers and their luggage from personal injury, loss or damage. To ensure that these objectives are attained in a digitized shipping environment, carriers must be held highly accountable so the strict liability regime should also extend to these types of incidents. Carriers and performing carriers must take all reasonable steps to provide a 'cyberworthy' vessel to avoid the stringent application of the Convention's liability regime especially knowing they will be presumed liable for such loss. *Article 4(2)* requires that the employer's servant or agent must have been acting within the scope of his employment. The phrase 'acting within the scope of his employment' means Alvin as an employee / crew member was operating under the instructions or supervision of his employer, carrying out his normal routine or work considered part of his job description. The facts are that Alvin was on his lunch break and in the process of playing his personal music when the incident occurred. It was not an instruction given by his employees neither was this akin to the nature of his employment. Does this mean that the carrier and performing carrier will not be held responsible for the actions of Alvin? The legal liability established under *Article 4(2)* of the *Athens Convention* is rooted in the principle of vicarious liability where an employer will be held responsible for the tort of his employee committed during his employment. On that basis, the principles from vicarious liability cases are transferable to the interpretation of the phrase 'acting within the course of employment'. The application of this principle to admiralty case is illustrated in decisions as early as *Simpson v Thomson*[402] where the point was made that **'**The owner of a ship is liable to an action for damages, not because he is the owner, but because he is the employer of the captain and crew, whose negligence in the course of their employment occasioned the damage.'

c. Issues of vicarious liability

4.22. The decision in *WM Morrison Supermarket plc v Various Claimants*[403] discussed the tort of vicarious liability in relation to a data breach alleged to be the result of a disgruntled employee who deliberately posted the payroll information of his colleagues online which exposed very sensitive personal details including the names, date of birth, addresses, national insurance number,

[402] (1887) 3 App Cas 279, 293.
[403] [2018] All ER (D) 89.

bank account number, sort code and the salary earned by each employee. The employee received the data on an encrypted USB flash drive; however, he copied the data to his personal USB with the intention of executing his malicious act. He later distributed the data to three different news outlets all of whom refused to publish the data but instead contacted Morrisons Supermarket and informed them about the website. Morrisons took immediate steps to remove the website. A class action was brought by the injured employees against Morrisons. In defence., Morrisons denied liability by arguing the employee was not acting in the course of his employment neither should Morrisons be held liable for the actions of an employee which caused harm to his employer. In assessing whether the employee was acting within the course of his employment, the issue 'whether there was a sufficient connection between Mr Skelton's employment and his wrongful conduct to make it right for Morrisons to be held vicariously liable?'

4.23. Reference was made to Mahmoud[404] where vicarious liability principles were discussed. In deciding whether Morrisons Supermarket was liable for the tort of their pump attendant who assaulted Mr. Mahmoud, the court decided that the test was to first ask 'what functions had been entrusted by the employer to the employee and secondly decide whether there was sufficient connection between the position in which he was employed and his wrongful conduct to make it right for the employer to be held liable.'[405] Alvin was at work but on his lunch break when the incident occurred so initial thought would be that he was on his own time on 'a frolic of his own'. However as was expressed in *WM Morrisons v Various Claimants*, 'the time and place at which the act occurred is relevant but not conclusive'[406] so the fact that Alvin was on his break will not completely shift where liability lies. Conversely, it is possible to argue that it should be in the contemplation of the employers that crew members while on their lunch break would seek comfort and convenience through personal entertainment, thus if they wanted to prevent any such occurrence proper measures should have been instituted to prevent crew members access to the general system and from connecting their USB and other personal devices directly to the vessel. Even if such standards were maintained or policies were implemented, CCL should be prepared

[404] *Mr A M Mohamud (in substitution for Mr A Mohamud (deceased)) (Appellant) v WM Morrison Supermarkets plc (Respondent*) [2016] UKSC 11.
[405] *Ibid,* [44] - [45].
[406] [2018] All ER (D) 89 [71].

that some employees will disobey the rules, therefore the best approach is to protect ship and offshore networks through effective network segregation[407] and proper procedures should be in place for the use of removeable media such as USB devices by ensuring that all devices are scanned for malware, encrypted, software maintenance in accordance with the International Safety Management Code, boundary protection devices are used and ports made unusable or physically locked especially where sensitive data are contained.[408] The vulnerability of administrative and crew welfare systems through which crew members accessed the internet was mentioned in the Guidelines where it was warned that they can be exploited to gain access to onboard systems and very valuable data. Accordingly, it is recommended that such systems along with guest entertainment systems which are considered uncontrolled should not be connected to any critical safety systems onboard.[409] These issues should all be addressed and recommendations form part of the ship's security management system. Notwithstanding the opportunity given to plug the flash in the system, that is not sufficient to establish vicarious liability especially when Alvin was on his personal time and pleasure.[410]

4.24. Even if Alvin had a paid lunch break or was still on the job completing his assigned tasks, that on its own would not meet the close connection test between the position in which he was employed and his negligent conduct so that CCL should be held liable. The facts do not suggest that Alvin's role required him to be in possession or have access to segments of the network storing the sensitive personal data of passengers and crew of CCL. The unintentional acts of Alvin are immaterial as his motive has no weight in determining whether the employers should be held vicariously liable. The employer WM Morrison Supermarket was not vicariously liable for the act

[407]Bimco and others, 'The Guidelines on Cyber Security Onboard Ships: Version 4' (Annex 4, 2020) p. 31 -32 <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships> accessed 22 September 2022.; IACS, 'Recommendation no. 166 on Cyber Resilience' (April 2020) (Corr.1. July 2020) 7.3.6(6) < https://iacs.org.uk/publications/recommendations/161-180/rec-166-new-corr1/> accessed 18 September 2022. 'Separation of networks supporting IT systems (e.g., for administrative tasks, passenger and crew connectivity, etc), OT systems (e.g., for engine control, cargo control, etc) and alarm systems'.

[408]Ibid IACS 7.3.5.3 (3) and 7.3.5.4 (2) <https://iacs.org.uk/publications/recommendations/161-180/rec-166-new-corr1/> accessed 18 September 2022.

[409]Bimco and others, 'The Guidelines on Cyber Security Onboard Ships: Version 4' (Annex 4, 2020) 19 <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships> accessed 22 September 2022.

[410] *WM Morrison Supermarkets plc (Appellant) v Various Claimants (Respondents)* [2020] UKSC 12, paras 32-47.

of his employee, Skelton who publicly disclosed the data. His authorised task was to transmit the data to the auditors thus his wrongful acts cannot be said to be so closely connected to his authorised task that it would be fair and proper to conclude that acting in the ordinary course of his employment.[411]

4.25. Based on the foregoing, the data breach onboard Santa Maria would not be categorised as a shipping incident, so CCL would not be held strictly liable to the passengers for the breach if they were to submit their claims under the Athens Convention and Protocol 2002. Accordingly, though the shipowners would have insurance[412], their P&I insurers would not be liable to indemnify the passengers for their distress or other loss from the data breach. It is unlikely that Alvin's action would be regarded as acts committed 'in the course of employment' so that CCL would not be held vicarious liable for Alvin's negligence. Despite this unfavourable conclusion for the passengers, all is not lost since it is still possible for a claim to be made under the fault based non shipping incident regime of the Athens Convention.

d. Non-shipping incident

4.26. Article 3(2) as amended by the Protocol of 2002 provides that the carrier will be liable for the death or personal injury to passenger which was not caused by a shipping incident if the incident which caused the loss was due to the fault or neglect of the carrier. Since the conclusion above is that the data breach is not a shipping incident, the claimants would have the burden of proving fault or neglect of the carrier, in this case CCL. Fault or neglect of the carrier has been interpreted as having the same meaning as negligence in common law.[413] There were obvious breaches or omission on the part of Santa Maria's management and IT personnel .to ensure that crew members were advised not to connect their personal devices onto the vessel's internet. They failed to put precautionary measures in place in the event of a breach of protocol by an employee

[411] Ibid.
[412] Article 4bis, Protocol to Athens Convention 2002. Article 4bis (10) allows the passengers to directly pursue claims for loss covered under the Convention against the insurer who has the right to limit his liability to no less than 250,000 units of account per passenger on each distinct occasion and may do so even when the carrier loses the right to limit his liability.
[413] Davis v Stena Line [2005] EWHC 420 (QB).

who chose to use his personal device despite instructions against such practices. Precautionary measures would include segregating the networks and installing systems to keep all data secured and, in a manner, that crew access to the network and any virus introduced by such access could not affect the entire system. CCL should have implemented procedures where it was compulsory for all devices to be scanned in an isolated computer before they can connect to the vessel's network. Additionally, CCL failed to ensure that crew was educated on system vulnerabilities and the risk of using personal devices to connect to the systems onboard the vessel. CCL also failed to ensure that the systems were encrypted, and firewalls put in place so there could be no access to passenger data. It is reasonable to conclude that the injury and damage suffered by the company and passengers was due to the negligence and fault of CCL.

4.27. The preceding establishes that it is likely that CCL will be held responsible for the damages to the victims of the data breach under the Athens Convention. If found liable under the *Athens Convention*, the carrier and performing carrier will be able to limit their liability to a maximum of 400 000 units of accounts per passenger on each distinct occasion of personal injury.[414] Article 14 prevents the passengers from bringing any action outside the Athens regime against the carrier or performing carrier for damages for the death of or personal injury to a passenger. The only exception is a contribution claim.[415] However, the Athens Convention was an international agreement on 'certain rules relating to the carriage or passengers and their luggage by sea' thus it is not comprehensive and will not apply to every conflict or association between the passengers their luggage and the carrier.[416] The Athens Conventions and its Protocol of 2002 certainly do not regulate privacy rights and data protection of its crew and passengers, consequently the passenger or crew member who is a victim of breach due to the negligence of the carrier should be allowed to bring an action against the carrier outside the realms of the Convention. Hence the discussion which follows. These arguments are reinforced by the Athens 2002 PLR Extension Clause which incorporates CL.380 to exempt the insurers from liability for loss or damage from a cyber-

[414] Article 7 (1) Athens Convention.
[415] *South West SHA v Bay Island Voyages* [2015] EWCA Civ 708.
[416] Abnett v British Airways Plc [1997] A.C. 430; [1996] 12 WLUK 269.

attack.[417] With the incorporation of CL.380 to the policy, the insurers would undoubtedly be exempted from any liability from the cyber-attack to passengers and crew.

D. Liability under the regulatory regime on data breach: GDPR / DPA 2018

a. Real life Case Studies: ICO response to data breaches

4.28. Considering that the incident occurred in 2019, the applicable data protection legislation is the *GDPR* which came into force on 25 May 2018. *The Data Protection Act 2018* incorporates the *GDPR* into domestic laws of England and Wales. The ICO is the supervisory body responsible for the monitoring the application of the data protection legislation with powers to issue administrative fines, to request information from controllers and processors and to carry out data protection audits among other functions.[418] CCL has breached *section 91 of the DPA 2018,* particularly data principle 6 which places an obligation on the data processor to ensure that personal data is processed in a manner that includes appropriate security measures having regard to the risks that arise from the processing of such data.[419] The type of risks that should be considered and measures taken to prevent, include 'the accidental or unauthorised access to, or destruction, loss, use, modification or disclosure of personal data.'[420] CCL did not institute effective security measures to prevent the loss, destruction and unauthorized access of the personal data of their passengers and employees. This is an egregious violation of the data protection legislation and the privacy rights of the data subjects. Consequently, the suitable penalty for failure to comply with *section 91 of the DPA 2018* is the higher maximum amount[421] which 'in the case of an undertaking, £17,500,000 or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher or in any other case, £17,500,000.'[422] The amount that is imposed by the ICO for a breach will depend on the nature, gravity and duration of the

[417] UKP&I, 'Rulebook 2022' (Appendix I, 1A.2(c))
< https://www.ukpandi.com/news-and-resources/rulebook-2022?chapter=appendix+i+clauses> accessed 19 September 2022.
[418] DPA 2018, section 115.
[419] Data Protection Act 2018, section 91 (i).
[420] DPA, section 91 (ii).
[421] DPA 2018, section 157 (3) (a).
[422] DPA 2018, section 157 (5) ; UK GDPR 2018, Article 83 (5)

infringement, taking into account the nature, scope or purpose of the processing as well as the number of data subjects affected and the level of damage suffered. Whether the act which led to the breach was intentional or negligent will also influence the amount to be imposed as a fine. The mitigating efforts of the controller or processor and previous infringements by the data controller will be considered when determining the fine that should be imposed.[423] The overall objective is to make sure that the fine imposed is effective, proportionate and dissuasive[424].

4.29. There have been incidents of data breach which the UK's (ICO) presided over, and the marine sector is not more immune than any other sector to this type of risk. Some of the major data breaches that have occurred within the UK (in wider business areas as examples) include the attacks against Morrisons Supermarket, Dixons (Carphone Warehouse), British Airways (BA), Equifax, Yahoo and Jala Transport. The attack on BA is evidence that the transportation sector is a lucrative target for cyber criminals and the equivalent in the marine sector would be a passenger vessel such as Santa Maria which host thousands of passengers annually. These incidents had penalties imposed for data breach ranging from Equifax maximum penalty of £500,000[425] under the UK DPA 1998 to BA being issued a notice of intent of a fine of £183.39 million which was reduced to a final settlement of £20 million after the ICO considered representations from BA and the economic impact of COVID-19 on the business.[426] A similar notice of intent to impose a fine of £99,200,396 million on Marriott International hotel chain, 3 % of the company's turnover was

[423] See Article 83 (2) (a) –(k) UK GDPR 2018; section 155 (2) and (3) DPA 2018. Other factors include "the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them ; the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement" inter alia.

[424] Article 83 (1) GDPR.

[425] ICO, 'Information Commissioner's Annual Report and Financial Statements 2018 -2019' (08 July 2019) p.24 < https://ico.org.uk/media/about-the-ico/documents/4017979/annual-report-201819.pdf> accessed 24 September 2022.

[426] ICO, 'Penalty Notice Section 155 Data Protection Act 2018: Case ref COM0783542 British Airways plc' (16 October 2020) paras 1.7., 2.15., 3.25., 7.53.,7.55. and 7.123. < https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf> accessed 24 September 2022.

also issued by the ICO[427] and reduced to a £18.4 million fine having considered multiple mitigating factors and the impact of COVID-19.[428]

4.30. The NotPetya virus attack destroyed all of Maersk end user devices, including 49,000 laptops and print capability, all 1,200 applications were inaccessible and approximately 1,000 destroyed. More than half of the 6,200 servers were destroyed and could not be reinstalled yet despite the operational and communication disruptions, there was no evidence of data breach or data loss.[429] The rapid proliferation of the virus crippled Maersk container shipping and brought to halt various port systems around the world. It was one of the first major cyber- attack on a large shipping company that was made public. The time of the attack is significant, it coincided with a period of intensified support for the enactment of more stringent data privacy legislation and the need for companies to be more transparent about actual and suspected data breaches. Such atmosphere undoubtedly placed immense pressure on Maersk to disclose details about the breach. In the end, not much is known about the final insurance settlement, but the scale of damage was massive even though not as grave as it could potentially have been. Whereas the ICO did not rule on this incident, it is a case worthy of mention because it demonstrates how easily a virus can proliferate within the database of a shipping company and the extensive damages and costs directly and indirectly caused by such security / data breach.

II. Insurance Implications of Santa Maria Data Breach

A. Insurability of fine: GDPR / DPA 2018

4.31. There is no formal statement from the ICO or any other legal entity with Jurisdiction on this issue that have addressed the question of whether fines and penalties imposed under the *DPA*

[427] DLA Piper and Aon, 'The price of data security: the insurability of GDPR fines across Europe' (3rd edn, May 2020) 5 <https://www.dlapiper.com/en/uk/insights/publications/2020/05/third-edition-of-guide-on-the-insurability-of-gdpr-fines-across-europe/> accessed 24 September 2022.

[428] ICO, 'Penalty Notice Section 155, Data Protection Act 2018:Case ref COM0804337 Marriott International Inc' (30 October 2020 paras 1.7, 5.3 < https://ico.org.uk/action-weve-taken/enforcement/marriott-international-inc/> accessed 24 September 2022.

[429] Rae Ritchie, 'Maersk: Springing back from a catastrophic cyber-attack' (Adam Banks speaking at Infosecurity Europe August 2019)
< https://mfame.guru/maersk-springing-back-from-notpetya-attack/ k> accessed 22 September 2022.

and *GDPR 2018* are insurable. As a result, there is uncertainty among not only the insurers but more so assureds who face the risk of having to pay these fines or penalties out of pocket. This situation is in direct contrast to the position under the Financial Conduct Authority, where there is explicit prohibition of the insurance of fines it has imposed for any breach of the financial regulations. Chapter 6 of the *General Provisions module of the FCA Handbook* (GEN) contains rules prohibiting a firm or member from entering into, arranging, claiming on or making a payment under a contract of insurance that is intended to have or has the effect of indemnifying any person against a financial penalty.[430] *Rule 1.5.33 in the FCA's Prudential Sourcebook* for insurers prohibits a long term insurer (including a firm qualifying for authorization under schedule 3 r 4 to the Act), which is not mutual, from paying a financial penalty from a long term insurance fund.[431] The debate as to the insurability of a fine rests substantially on the wording of the policy or principle of illegality / ex turpi causa maxim as developed in the judgment of *Lord Mansfield CJ* in *Holman v Johnson* 'No court will lend its aid to a man who found his cause of action on an immoral or illegal act.'[432] and later in *Gray v Thames Trains Ltd*[433] where *Lord Hoffman* said '… It would be inconsistent with public policy for a civil court to award damages to the claimant for a criminal or negligent act for which he is responsible.'[434]

4.32. Some insurance policies will deny cover for fines or penalties. On the other hand, some policies will only refuse insurance for criminal fines. The expression which often appears in cyber policies is that 'fines are covered to the extent that they are insurable by law', an expression which means very little when the law in the country of policy is silent on the issue. Other policy provides that the insurability of the fines shall be determined by the laws of any applicable jurisdiction that most favours coverage for such monetary fines or penalties. Reproduced below are examples of such a clause as can be found in some cyber insurance policies:

---

[430] Financial Conduct Authority, 'GEN.1 Payment of Financial Penalty' (Updated 14/04/22).
< https://www.handbook.fca.org.uk/handbook/GEN/6/?view=chapter > accessed 24 September 2022.
[431] Financial Conduct Authority, 'INSPRU 1.5.33: Payment of Financial Penalties'
< https://www.handbook.fca.org.uk/handbook/INSPRU/1/?view=chapter> accessed 24 September 2022.
[432] 98 E.R. 1120; (1775) 1 Cowp. 341.
[433] [2009] 1 AC 1339.
[434] [2009] 1 AC 1339 [29], [32].

Tokio Marine HCC - Cyber Security Policy Wording 0417[435]

1.5 Regulatory defence and penalties

The Insurer agrees to indemnify the Insured for..., **civil penalty or fines to the extent insurable by law imposed against the Insured** by a government or public authority charged with the regulation of the control of Personal information …
Provided that the Insurer's maximum liability will not exceed GBP 250,000 in respect of any one Claim and in total for all Claims first made during the Period of insurance.

Zurich Cyber Policy[436]
Section A. 11. Civil fines and penalties

We will reimburse you for civil fines and penalties, including those arising out of the General Data Protection Regulation (GDPR), which you become liable to pay as a result of a privacy event provided that such privacy event is first discovered and notified to us during the period of insurance.

Hiscox CyberClear[437]

"What is not covered
B. **We will** not make any payment for:
1. …..
2. …..
3. Fines, penalties and sanctions
   Criminals, civil or regulatory sanctions, fines, penalties, … including but not limited to those imposed by any national or local governmental body or any licensing organisation.

   However, this exclusion does not apply for:
   a. PCI charges; or
   b. Regulatory awards

SIGCO Cyber Hull Insurance[438]

[435] Tokio Marine HCC, 'Professional Risks Cyber Security Policy Wording 0417: Regulatory defence and penalties'' (October 2017) <https://www.tmhcc.com/-/media/RoW/Documents/PI/Cyber/Cyber-Security-Insurance-Wording-0417.pdf >accessed 24 September 2022.

[436] Zurich Insurance plc, 'Cyber Policy: Section A – Cyber Cover Clause 11 ' SME513C.04 (NP721418004) (10/20) CMS accessed <https://www.zurich.co.uk/business/business-insurance/specialty-lines/financial-lines/cyber> accessed 24 September 2022.

[437] Hiscox Cyber Clear Policy, 'WD-PIP-UK-CCLEAR (1) 19029 12/18' (2018) <https://www.hiscox.co.uk/sites/uk/files/documents/2019-03/19029-CyberClear-policy-wording.pdf> accessed September 2022.

[438] SIGCo Group, 'Cyber Hull Insurance' (v4- 21 July 2021) < https://www.sigcogroup.com/docs/Policy_Wording_Revised_v1.4.pdf> accessed 21 September 2022.

5.1 Exclusions to Insuring Agreement
This insurance shall not cover:
…
5.1.11 punitive or exemplary damages, or fines or penalties of any nature.
5.1.12 matters that may be deemed uninsurable under the law pursuant to which this Policy may be construed.
…

The position across Europe on the insurability of GDPR fines is not uniform.[439] It is unlikely that GDPR fines will be insurable in the UK and it is not expected that administrative fines will fall into case law exceptions to the public policy rule against the insurance of fines.[440] Even though the insurability of administrative fines may differ across states, it is generally accepted that fines imposed for criminal offenses under the *DPA 2018* will not be insurable.[441] Despite the difference in opinion and laws on the insurability of fines across states, a common theme in cyber insurance policies is cover for the reasonable and necessary lawyer and expert fees incurred to investigate, defend, appeal and settle a data breach. So, whereas the fine imposed by the UK ICO may not be insurable, the defence costs relating to such fine is insurable.[442] An example of this clause is Clause 3 of Zurich Cyber Policy:

Regulatory proceeding defence costs[443]

"We will reimburse all reasonable charges, costs, expenses and fees necessarily incurred with our written consent which the insured incurs in respect of any regulatory proceeding first taken

[439] Aon and DLA Piper, 'The price of data security- A guide to the insurability of GDPR fines across Europe' (3rd edn May 2020) pages 12-26 <https://www.aon.com/unitedkingdom/insights/a-guide-to-the-insurability-of-gdpr-fine.jsp> accessed 24 September 2022 . Most EU states believe that due to public policy reasons, fines and penalties imposed by the regulatory body with authority under the GDPR will not be insurable. In Greece for example, it is likely that fines will be insurable provided they are not attributable to malice or are criminal offenses. Conversely, Finland's Financial Advisory Authority in 2018 rejected the notion of the insurability of GDPR fines by stating that granting insurance cover for fines and penalties is against good insurance practice. Other states, for example the Czech Republic, remain silent on the issue consequently the outcome may end in any direction.

[440] Ibid 25. Other costs following the data breach are insurable such as: investigation and defence costs, third party costs and mitigating costs including public relations expenses provided the fine was not the result of the reckless or deliberate act of the assured.

[441] Ibid.

[442] DLA Piper and Aon, 'The price of data security: the insurability of GDPR fines across Europe' (3rd edn, May 2020) 5 <https://www.dlapiper.com/en/uk/insights/publications/2020/05/third-edition-of-guide-on-the-insurability-of-gdpr-fines-across-europe/> accessed 24 September 2022. Makes the same point.
ee n571 (Aon and DLA Piper) which makes the same point.

[443] Zurich Insurance plc, 'Cyber Policy: Section A – Cyber Cover Clause 3 ' SME513C.04 (NP721418004) (10/20) CMS Available at: https://www.zurich.co.uk/business/business-insurance/specialty-lines/financial-lines/cyber Accessed 24 September 2022.

against the insured and notified to us during the period of insurance for a privacy wrongful act or security wrongful act provided that such privacy wrongful act or security wrongful act first occurs on or after the Retroactive Date stated in the schedule and is discovered during the period of insurance."

4.33. Fines are costs which P&I clubs agree to cover but under specific circumstances.[444] The fine or penalty must be incurred in direct connection with the operation of the vessel, in respect of the member's interest and from an incident which occurred while the Ship was entered in the P&I club.[445] These tend to be fines or penalties imposed upon a member and not the ship by a court, tribunal or other authority of competent jurisdiction regarding inaccuracies with cargo delivery declaration and documentation, breach of immigration law or regulations, or the threat or accidental escape or discharge of oil or any other substance.[446] The Club may exercise their discretion in covering other fines or penalties other than those listed, if CCL, by providing the relevant information, documentation and assistance with the Club's investigation can satisfy the Club that reasonable steps were taken to avoid the event giving rise to the fine or penalty.[447] Generally, P&I clubs have not excluded data protection liabilities from their cover, which by now they have had numerous opportunities to amend their Rules if that was intended. Though not necessarily, the typical P&I liabilities without directly excluding GDPR liabilities and fines, there is no reason why they cannot form part of the people claims for personal injury and fines already

[444] For a more detailed commentary on P&I rules on fines see Steven J Hazelwood and David Semark, *P&I Clubs Law and Practice* (4th edn, Informa 2010), paras 10.175 – 10-197; Richard Williams, *Gard Guidance on Maritime Claims and Insurance* (Gard AS, 2013), Chapter 8: Fines and Criminal Sanctions Claims.

[445] Gard Guidance to the Rules 2022 Risks covered- Rule 47: Fines (2021); Rule 2.4 <https://www.gard.no/web/publications/document/20747880/gard-guidance-to-the-rules-2022> accessed 24 September 2022. 'This is said to be based on a 'model rule' agreed between P&I clubs that are parties to the Pooling Agreement. The rule is designed to strike a balance between accidental or non-deliberate law infringements that are considered difficult to avoid given the trading environment in which ships normally operate and which are to be considered mutual risks that should be shared by members and ii) those infringements that a Member should have taken steps to avoid and which are not considered to be mutual risks but risks that should be for the Member's own account.' Cover for fines relating to cargo and the escape of oil or any other substance is conditional on the member being insured by the Association for cargo liability under Rule34 and pollution liability under Rule 38.

[446] Gard, 'P&I Club Rules 2022: Rule 47.1(a) –(c)' <https://www.gard.no/web/publications/document/chapter?p_subdoc_id=1070567&p_document_id=781871> accessed 24 September 2022.

[447] Gard, 'P&I Club Rules 2022: Rule 47.2(N)' ; Rules 82.2.d and e. <https://www.gard.no/web/publications/document/chapter?p_subdoc_id=1070567&p_document_id=781871> accessed 24 September 2022.

covered by P&I clubs.[448] As concluded above, CCL did not implement adequate and reasonable measures to prevent a successful attack of this nature on the company. Given that CCL would find it difficult to fulfil this proviso, it is improbable that their P&I insurers would pay any fines imposed by the ICO for breach of UK GDPR / DPA 2018.[449] Even if CCL had taken all reasonable steps to prevent the breach, the Club may choose not to cover the fine if the nature of the breach was such that it would be contrary to the interests of the membership as a whole.[450] It is unlikely that a data breach of the kind that occurred onboard Santa Maria particularly when reasonable measures were taken by CCL to avoid the breach including the training of employees and segregation of networks would warrant such a decision by the Club. However, if CCL blatantly ignored the cyber security guidelines, failed to implement an adequate security management system, and repeatedly contravenes the Data Protection Legislation, it would be reasonable and legitimate for board to refuse to exercise their discretion in covering fines imposed by the ICO, court or any other competent authority. It would be in the interest of the membership as a whole to discourage disregard of the rules and poor cyber security management practices onshore at company offices and onboard vessels. The Club will in some instances depending on the employment contract be required to indemnify the shipowners for a fine paid on behalf of a crew members whose acts or omission which led to the imposition of a fine or penalty was committed within the scope of his employment and duties onboard the vessel.[451]

4.34. The Supreme Court in *Les Laboratoires Servier and another (Apellants) v Apotex Inc and others (Respondents)*, considered the illegality point raised in defence to the claim. The point was

[448] North, 'FAQS: General Data Protection Regulation (GDPR) (January 2018), para 27.
< https://www.nepia.com/search?q=gdpr+faqs> accessed 24 September 2022.
[449] Some P&I clubs exclude cover unless the Board decides otherwise in respect of fines imposed arising from any personal act or default on the part of the member of his managers. The P&I insurers of CCL may rely on a similar exclusion if expressly included in their Rules. Overloading, illegal fishing and wilful misconduct on the part of any person unless the member has been compelled by law to pay the fine are also sometimes excluded from the rules on the recovery of fines.
Standard Club, 'Rule Book 2022/23 P&I Rules: Fines Rule 3.16' (2022) < https://www.standard-club.com/rules/rules-2022-2023/> accessed 24 September 2022.
[450] Gard, 'P&I Club Rules 2022: Rule 47.2(N)'
<https://www.gard.no/web/publications/document/chapter?p_subdoc_id=1070567&p_document_id=781871> accessed 24 September 2022.
[451] ibid Rule 47.2(C)'

that it was contrary to public policy for Apotex to recover damages for being prevented from selling a product whose manufacture in Canada would have been illegal as an infringement of Servier's Canada patent. One of the main issues which affected the judgment in the lower court was whether the infringement of a foreign patent rights constitute a relevant illegality for the purpose of the defence'[452] The next question is what constitutes a relevant illegality? Would a breach of the DPA 2018 be considered a relevant illegality to raise such a defence? The Court of Appeal in Euro- Diam v Bathurst Ltd per Kerr LJ said the test was whether ' in all the circumstances it would be an afront to the public conscience to grant the plaintiff the relief which he seeks because the court would thereby appear to assist or encourage the plaintiff in his illegal conduct or to encourage others in similar acts'.[453] In deciding what constitutes illegality or turpitude, the Supreme Court stated that though most of the authorities on this issue focused on criminal offenses, there are other types of behaviour which will be considered 'illegal or immoral'. These include 'acts which engage the interest of the state or the public interest'[454] Certainly, the *DPA 2018* concerns issues of public interest as it is intended to protect the privacy rights of individuals to prevent the unauthorized access and use of their personal identification information for fraudulent and other dishonest engagements. Besides criminal offenses and prohibited contracts, there are other quasi criminal acts which would trigger the operation of the defence, these include cases of dishonesty or corruption and the infringement of statutory rules that were designed to protect public interest and to which a penal sanction is applied if its terms are violated for example the competition law considered in Safeway Stores Ltd v Twigger.[455] By definition, an act that is merely tortious and affecting only the private individual will not constitute an illegal act that will allow for the ex turpi causa defence since it does not affect public interest. This is the conclusion arrived at in *Les Labarotoires Servier and another v Apotex Inc and others*, the illegality defence would not arise in breach of the Servier's Canadian patent because it was not an issue of public interest, it concerned only the rights of the patentee.

[452] [2014] UKSC 55 [9].
[453] [1990] 1 B 1, 35.
[454] [2014] UKSC 55[23]
[455] *[2010] 3 All ER 577*

4.35. The general position in the UK is that fines from intentional wrongdoing, fraudulent behaviour and dishonesty will not be indemnifiable. Conversely in strict liability provisions, it is likely that the fines will be indemnifiable as there is no requirement that the assureds conduct is immoral or illegal. This is subject to whether the regulations / legislation prohibits the insurance of any fine or penalty levied under its authority. Where an act is considered negligent, the insurability of the fine or penalty will depend on whether it was an innocent or deliberate and intentional act. In the former, it is unlikely that the illegality defence will be triggered whereas in the latter, it is more likely that the defence will operate to deny the claimant of any indemnification for his conduct.[456] Accordingly, a decision of whether a fine or penalty is insurable will depend significantly on the morality involved in the conduct which directly or indirectly causes the infringement. However, there may be the absence of moral turpitude yet the fine or penalty is uninsurable based on prohibition by the rule of law applicable to the situation or based on concerns of public policy.

4.36. If this reasoning is to be applied to the provisions of the UK GDPR, the fines or penalties that are associated with conduct deemed to be criminal by the regulation will not be insurable. This relates specifically to the offenses of 'intentionally or recklessly reidentifying individuals from anonymised data and altering records with the intention of preventing disclosure of that information due to a subject access request pursuant to the *DPA 2018* will not be insurable. Even conduct which does not qualify as criminal, if performed negligently or recklessly may become uninsurable based on the public policy issues. As it relates to administrative fines under Article 83(2) of the UK GDR, the regulator being ICO will need to consider the negligent or intentional conduct which constituted the breach, the severity and duration of the breach and security history of the company, the type of data exposed and whether the breach affected the rights and freedoms

[456] Helen Bourne and Henning Schaloske, 'Insurability of fines and penalties for breaches of the GDPR: A UK and German Perspective' (30 January 2019) < https://www.clydeco.com/blog/insurance-hub/article/insurability-of-fines-and-penalties-for-breaches-of-the-gdpr-a-uk-and-germa> accessed 24 September 2022. Now accessible at <https://www.commercialriskonline.com/wp-content/uploads/2019/02/Insurability-of-fines-and-penalties-for-GDPR.pdf> accessed 24 September 2022.

of the data subjects involved inter alia. These are the factors which will contribute to the discussion and conclusion as to whether an administrative fine is insurable.

4.37. If we were to consider *section 41* of the *Marine insurance Act 1906*, there is an implied warranty of legality where it is expected that the Adventure is legal and the same applies for the execution of the adventure. Santa Maria has undertaken what in all respects appear to be a legal adventure, a passenger cruise with no underlying criminal, illegal or immoral motive. The question is whether the security breaches onboard would be considered a violation of the *ISM and ISPS Code* and thus constituted an illegal act fit to trigger the operation of the illegality warranty in section 41. If the reasoning from *Les Laboratoires* as to what constitutes illegality is to be applied, violation of the ISM *and ISPS codes* would be of public interest because it exposes many people, facilities and even national security to high level risks sufficient to be termed illegal or at the very least quasi criminal. This would mean that CCL marine insurance policy may be declared void due to the breach of the warranty of legality. That would be the position if the parties of the insurance contract decided to opt out of the warranty regime in *section 10* of the *Insurance Act 2015*, which revokes the position in the *MIA 1906, section 17* and implement the new law that a breach of a warranty will not automatically discharge the insurer of all liability under the contract of insurance. This reasoning is not one that would sit well with some stakeholders within the maritime industry. The *ISM and ISPS codes* were designed to protect and provide a safe regime for all those involved in shipping. It would be absurd and completely opposite to its object and purpose if any breach of its terms would be declared 'illegal' and of such moral turpitude to deny a shipowner his right to insurance. The ability of an assured to have access to insurance in the event of a safety breach is entrenched in the idea of protecting and providing a safe environment for all including passengers onboard passenger vessels. The practice has been that violation of safety regulations do not automatically render the voyage illegal, the issue will become one of seaworthiness and whether Santa Maria was seaworthy at the beginning of its voyage.[457] The denial of indemnity by the

[457] Baris Soyer*, Warranties in Marine Insurance* (3rd edn, Informa Law 2017) para 4.44; St. John Shipping Coro v Joseph Rank Ltd [1957] 1 QB 267.

insurers would more likely be due to the unseaworthiness of the vessel at the beginning of the journey rather than because of the breach of the ISM and ISPS codes.

4.38. In the present case, CCL is the assured against whom the principle would operate even though the negligent act was committed by Alvin. The law treats a company as legal entity however the company itself cannot commit a criminal or negligent act. Instead, its liability will depend on the actions or omissions of senior management who are the directing will and mind of the organization. The issue is whether CCL's failure to maintain the data principles under the DPA 2018 was intentionally or negligently committed, the response to which will determine their right to recovery from his insurers of any fine or penalty. If an assured could transfer his penalty to the insurers, the policy or mischief which the regulation / legislation was designed to resolve would lose its significance. The assured would have less incentive to ensure that procedures are put in place for the maximum observance and adherence to the data protection legislation if they were certain that their insurer would pay for the fine / penalty. In the case of CCL, they might think it is cheaper to get insurance rather than spend millions to continuously upgrade and manage their IT and operational systems and hire experts to keep abreast of the changing nature of cyber risk. Uncertainty will persist until a case or an industry guideline on data and privacy issues decide on the insurability of fines under the regulation and state unequivocally whether it is permitted. A common practice among insurers is to include a statement in the policy with these words 'the insurability of penalties will be in accordance with the law in the applicable venue that most favours coverage for such penalties.' The applicable law could be the law where the incident occurs, where each data subject, corporate entity or government affected by the breach is situated, head office of the assured and or his principal place of business. Whenever the question was raised to insurers, they tend to be unsure about the position in the UK, this suggest the clause exist to appease the assured but there is no guarantee of protection if and when a fine or penalty is imposed by the ICO. Once more, the assured is placed in an uncomfortable and uncertain position, CCL does not know and has no real guidance on whether they will be indemnified if fined by the ICO. A fine imposed by the ICO is a very likely result based on the cases, notices of intentions and the penalties already imposed by a very active ICO.

4.39. DLA Piper carried out study on the insurability of GDPR fines within Europe where the current law in each member state was discussed[458]. In majority of the EU states, the fines and penalties imposed by the regulatory body with authority under the GDPR will not be insurable based on the public policy reasons. There are however few exceptions, where fines under the GDPR may be insurable such as the position in Czech Republic and Greece. In Czech Republic, GDPR fines may be insurable as there is no express prohibition against same, but it is still possible that such contract may be declared unenforceable based on public policy reasons. In Greece, *GDPR* fines could be insurable if they are not attributable to malice and that the acts and omissions are not criminal offenses which resulted in criminal sanction. On the far end of the spectrum is Finland whose *Financial Supervisory Authority* has declared in 2018 that granting insurance fines are unlikely to be insurable in most cases. While there have been exceptions to the public policy rule that fines are insurable, it is unconvincing that the exception will be applied when deciding on the insurability of administrative fines under the *GDPR / DPA 2018*.[459] It is without doubt that fines imposed for criminal offenses under the *DPA 2018* will not be insurable. This is based on the general rule of law which prohibits indemnity for criminal or quasi-criminal offenses as the party in breach shall be personally held responsible.

III Insurance for Data Breach: Are they adequate?

A. Marine Insurance Policies and Data Breach

4.40. Traditional lines of marine insurance do not protect against the type of damages suffered in this scenario. Similarly, P & I clubs have made no mention of whether they will provide cover for data breaches and have not expressly excluded cyber risks.[460] As such, time will not be wasted on an extensive discussion of those policies. Instead, we will focus on some of the cyber policies that are available in the insurance market, many of which were not designed for the maritime sector

[458] Aon and DLA Piper, 'The price of data security- A guide to the insurability of GDPR fines across Europe' (3rd edn May 2020) <https://www.aon.com/unitedkingdom/insights/a-guide-to-the-insurability-of-gdpr-fine.jsp> accessed 24 September 2024.

[459] Ibid 12-26.

[460] See discussion in the scenario 1 on piracy as to whether 'data or software loss are classed as property under marine insurance policies. The general conclusion is that these policies do not treat data and software loss or damage as property so the insured will not be indemnified for such loss.

and few specifically designed to cover such risk among maritime assets. Essentially this means that an assured shipowner or carrier in **CCL's** position will probably not have any protection under his marine insurance policies as they will include the very popular and widely used **CL.380** or any variant thereof. Consequently, the most viable option is for insured in the maritime sector to invest in a cyber liability policy which will cover cyber related losses including data loss and the liabilities discussed above. We will briefly discuss three possible scenarios; first what will happen where the assured has a cyber exclusion clause in his policy, secondly when the assured marine insurance policy includes a cyber endorsement clause and thirdly where the assured has a standalone cyber insurance policy in addition to his traditional marine insurance policies.

a. Cyber Exclusions in Marine Insurance

i. CL.380: Institute Cyber Attack Exclusion Clause

4.41. *CL.380* was discussed above (scenario 1) but how does it operate under these circumstances where Alvin had no intention of causing harm? Alwin was unaware that the malware was on his flash drive which justifies the inference that his actions were not premeditated. He had no intention of causing harm to the company or anyone.

Paragraph 1.1 of *CL.380* will be repeated here for ease of reference'

> 1.1 Subject only to clause 1. 2 below, **in no case shall this** insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from **the use or operation, as a means for inflicting harm**, of any computer, computer system, computer software program, malicious code, computer virus or process or any other electronic system.

Since it is reasonable to infer a lack of intention on the part of Alvin to cause harm, does this mean that ***CL.380*** would not be applicable to this scenario? On initial reading, clause 1.1 may be interpreted as such, that the clause becomes operative only when an intention of harm can be proved. The problem here is that there is no guidance on whose intention needs to be established. In other words, will the court be interested in the Alvin's intention? The absence of which would prevent the application of the clause. Alternatively, where a malicious code or computer virus is used, is it correct to challenge the absence of an intention to inflict harm by suggesting that the

underlying intention or objective of the creator of the code or virus is to inflict harm? The better view is that the purpose or function that the code was designed to achieve should be the determinant and not necessarily the intention of the owner of the device who may or may not be privy to the existence of the virus. If the latter interpretation is accepted, *CL.380* would fully apply and relieve the insurers of any liability to CCL or other victims of the data breach. On the contrary, relying on the intention of the creator of the malicious code or virus to satisfy the requirement to 'use or operate as a means for inflicting harm' is giving the phrase a more extensive meaning than was intended since the words 'use or operate', indicate a step beyond the creation of the code, instead the emphasis is on how the code has been employed. Certainly, there are coders who develop viruses for credible and good causes such as its use by ethical hackers for penetration testing within an organization or across networks. When this is the case, the assumption that the creator had malicious intent is to be rejected and should not be relied on by insurers as the prompt for the operation of the exclusion clause. This is a complicated process primarily because it is often unknown the purpose for which a code or virus was written and the point at which a virus or code created for a good cause has been exploited and used to inflict harm. On another note, this position may be criticized for going beyond the literal meaning of the clause when there is no legal basis to do so. The clause itself is qualified by the word 'malicious' which indicates that harm was intended therefore there is no basis to argue the lack of intention to inflict harm. The presence of an intention to cause harm by the creator of the code or virus and the absence of either or both being used or operated to inflict harm should not be the reason for the application of exclusion clause. However, there is still uncertainty so assureds and insurers both await a court decision or practice direction to clarify the meaning and how exactly CL.380 should be interpreted especially when the intent to cause harm is not readily established.

ii. LMA5402: Marine Cyber Exclusion

4.42. The text of this clause reads;

> 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 program, malicious code, computer virus or process or any other electronic system.

A significant difference between LMA5402 and CL.380 is the pronouncement in the introductory sentence that the clause shall be paramount. Usually, any reference to a paramount clause in maritime law means that there is either the incorporation of the *Hague or Hague Visby Rules* into the contract of carriage depending on which version of the *Rules* is applicable in the country of shipment.[461] Describing the clause as paramount to any other clause in the insurance contract means that all ambiguities shall be removed as to the status of the clause especially where there is a conflict in interpretation. In other words, any clause of the insurance policy that conflicts or is inconsistent with the terms of clause 1.1 and 1.2 will be declared null and or the latter will take precedence over the contravening clause. CL.380 begin with the words 'Subject only to clause 1. 2 below, in no case shall this insurance cover', those words would be expected to have a status and effect akin to a paramount clause. Notwithstanding this perceived clarity, there is always the prospect that flaws may be found in the drafting of contractual terms especially where parties disagree as to the interpretation or initial intention of a clause. Importantly, the doubt or the risk of conflicting interpretation which may arise from the construction of CL.380 is reduced or completely removed by clarifying in LMA5402 that the clause takes precedence above every other clause in the policy.

4.43. Another distinction between LMA5402 and CL.380 is the division in the original clause 1.1 found in the latter. Whereas the text is quite similar, LMA5402 does not include the words as 'a means of inflicting harm' as a general requirement throughout. Instead, the drafter divided the

[461] *The Superior Pescadores Syemgas FZCO and Others v Superior Pescadores SA* [2016] EWCA Civ 101; *Bukhta Russkaya* [1997] 2 Lloyds Rep 744, 746: Thomas J explained the effect of a paramount clause as follows: '(1) if the Hague Rules are enacted in the country of shipment, then they apply as enacted; (2) if the Hague Rules are not enacted in the country of shipment, the corresponding legislation of the country of destination applies or, if there is no such legislation, the terms of the Convention containing the Hague Rules apply; (3) if the Hague-Visby Rules are compulsorily applicable to the trade in question, then the legislation enacting those rules applies.'

original CL.380 clause 1.1 into two parts, to recreate clause 1.1 and 1.2 of the LMA5402. This means that the exclusion clause becomes operative and is paramount in one of two situations either where there is a failure, error or malfunction of any computer, computer system, computer software program, code (which is new as it did not form part of the original CL.380 clause) OR the second situation is the use or operation, as a means for inflicting harm of any computer … computer virus or process or any electronic system. An important point here is the use of the word 'or' between clause 1.1 and 1.2 in LMA5402 whereas parts of both clauses would have formed the continuous prose of CL.380. This means that the clause 1.1 of LMA5402 removes the shortcomings of CL.380 where an assured may argue that their act was not deliberate and the systems, code, virus or device was not used or operated to inflict harm. The difficulty in finding the necessary intent or attributing the same on a party of the insurance policy is difficult especially because of the transient nature of cyber risks. Accordingly, as it relates to Alvin's situation if the LMA5402 was included in any of the marine insurance policies, the insurer may argue that even if they cannot satisfy the requirements of clause 1.2 in proving the virus was to inflict harm, if clause 1.1 is met then there is no further obligation on the part of the insurer to the assured. In defence, the words in clause 1.1 are 'failure, error, malfunction of a computer system'. Some will suggest that these words are so restricted in definition that there is no room for an extended interpretation to include a malicious code. A possible explanation is that failure, error, malfunction represents an internal or innate breakdown of the system not necessarily caused by a third party or something foreign. Another explanation is the phrase 'a failure, error or malfunction of a computer system' is a very generic and does not specify what should be the cause of either the error, failure or malfunction therefore it is very broad and could cover various type of scenarios. Interestingly, there is mention made of a 'code' in clause 1.1 of the LMA5402 without the preceding qualification of "'malicious' code" as found in clause 1.1 of CL.380. This was a deliberate omission by the drafters and is further support for the view that their aim was to exclude situations where there was no evidence of malicious intent. This means that the LMA5402 has room for wider interpretation and application than CL.380. Equally so, is the less uncertainty in the wording of the clause as insurers and assured are now fully aware that non-intentional breaches will also be excluded. On that basis, if CCL Hull or any other insurance policy incorporated this clause within the policy, the assureds could not

expect to be indemnified for the losses incurred as a result of the data breach which was inadvertently due to the actions of Alvin.

b. Cyber endorsement in Marine Insurance policies – Data Breach Protection

4.44. While most marine insurance policies will seek to incorporate either the CL.380 or LMA5402 to exclude computer related risks, there have been other developments in the sector, some insurers have made attempts to extend their cover to include an increasing degree of protection against cyber risks. This trend is in the form of cyber endorsements in traditional marine insurance policies, few of which will be discussed herein. This is partially due to the IMO requirement that as of 1 January 2021, all policies must clearly state whether cyber risk is covered or excluded.

A recent example of this type of clause is **LMA5403**- marine cyber endorsement below:

> 1 Subject only to paragraph 3 below, in **no case shall this insurance cover loss, damage, liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm**, of any computer, computer system, computer software programme, malicious code, computer virus, computer process or any other electronic system.
>
> 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.**
>
> 3 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, paragraph 1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

4.45. Interestingly, LMA5403 is an extension of CL.380 since clause 1 and 3 are the original paragraphs of CL.380. The only addition to LMA5403 is paragraph 2 which purports that:

> Subject to the conditions, limitations and exclusions to which the clause is attached, the assured will be indemnified for losses recoverable under the policy where caused by any computer system or computer software program, computer process or any other electronic system provided they were not used or operated as a means for inflicting harm.

Insurers are effectively offering a writeback for the exclusion in LMA5402 clause 1.1. With LMA5403, an assured in CCL's position may still experience some difficulty since there was a deliberate omission of the words 'malicious code or virus' in paragraph 2 thereby suggesting that the insurer is not prepared to cover liabilities directly or indirectly caused by the use or operation of a malicious code or virus even where no harm was intended. Otherwise, some proponents of the clause especially assureds who have the clause endorsed on for example their hull insurance policy and is in CCL's position will argue that "any computer, computer system…or electronic system" is wide enough to provide cover against the inadvertent actions of Alvin which led to the data breach. Many assureds will be relieved that they will be indemnified for losses resulting from the negligent, inadvertent act of their employees and or agent whose use or operation of the computer system, computer software programme or computer processes was not to inflict harm.

B. Cyber insurance and data breach

4.46. The third option for CCL would be to seek reimbursement for the losses incurred from his cyber liability insurers provided they had a policy in place during the period of the incident. Here, the researcher will examine two types of cyber insurance policies; those designed specifically for the marine industry and the more general data liability insurance. This will be done to aid with the analysis of whether either of policies would adequately protect and indemnify CCL against the risks and liabilities which may arise from the data breach onboard Santa Maria. It will be assumed that CCL purchased insurance from each of these insurers.

a. Marine Cyber Insurance Policy

i. Defining the breadth of the cover- The Insuring Clause

4.47. In the first clause labelled 'Insuring Clause', SIGCo set out that they will provide cover for the popular CL.380 exclusion clause. The technique is engrossing to any shipowner however this is subject to limitation, exclusions and conditions within the policy which means there is no absolute protection against losses caused by a computer, computer system used or operated to inflict harm. The meaning of cyber-attack is defined in clause 6.5:

> **6.5 Cyber Attack** means 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 by any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organization (s) and whether or not induced by the use of force or violence or threat thereof to commit such acts, and which directly or indirectly **results in actual physical loss or damage to the Vessel or liability of the Vessel.**[462]

The analysis will begin with clause 6.5 where cyber-attack has been defined by the insurers. It is to be noted that an event will only be considered a cyber-attack if it directly or indirectly results in physical loss or damage to the vessel or liability of the vessel. The emphasis by the insurers on physical loss or damage is indicative of their reluctance to cover data breaches and the losses suffered by CCL and its passengers which are not typically categorized as physical loss or damage by the insurance sector. Accordingly, the data breach would not be classified as a cyber-attack under the SIGCo policy and the basis on which the insurers would deny liability for the loss. The position of the CCL would become more dire when focus is placed on the exclusion clauses within the policy.

Exclusions

4.48. The exclusion clause begins at Clause 5.1 with the heading "Exclusions to Insuring Agreement'. The insurance shall not cover:[463]

> Clause 5.1.1 costs of updating or upgrading the Assured vessel.
>
> Clause 5.1.2 costs of repairing, recreating, gathering or assembling an electronic data or computer software, or the repair or replacement of any parts or components of any computer hardware.
>
> Clause 5.1.3 other than Collision Liabilities, any form of third party liability or other legal liability, including but not limited to, any lawsuits, claims or demands by any third party or by any Employee, officer, director or partner of the Assured
>
> Clause 5.1.8 the economic or market value of data
>
> Clause 5.1.11 punitive or exemplary damages, or fines or penalties of any nature

[462] SIGCo Group, 'Cyber Insurance' (v4- 21 July 2021)
< https://www.sigcogroup.com/docs/Policy_Wording_Revised_v1.4.pdf> accessed 24 September 2022.
[463] The list is long ranging from clause 5.1.1 – 5.1.22.7, so mention will only be made of those exclusions most relevant to the scenario.

6.3.3 loss of life, personal injury or illness

……..

Based on the exclusions, the insurers are not prepared to cover the cost for any repairs, assembling, replacement of any electronic data nor are they willing to cover the cost of repairs to any computer software or hardware. So even with this policy in place, CCL would not be indemnified for the data loss and for the damage to the computer system due to the breach. Consequently, data replacement costs would have to be paid out of pocket by the owners. A data breach onboard a cruise vessel that exposes both personal and company data could easily cost millions to repair or replace if possible so this will be a strain economically on CCL.

Third Party Liability

4.49. Clause 5.1.3 exempts the insurer from any third-party liability which includes legal suits and claims from employees, shareholders, directors and partners of the company. Essentially, this means that with a SIGCo v4 policy, if the shareholders or employees of CCL were to initiate a class action[464] or pursue individual claims against CCL for loss due to the data breach, CCL request to the insurers to be indemnified for such claims or be subrogated in these matters would be rejected. This would place CCL in another precarious position as they would need to find an alternative source or another insurer (P&I) to cover the potential claims.

Fines and Penalties

4.50. In addition to this, the insurers have excluded in clause 5.1.11 any punitive or exemplary damages, fines or penalties of any nature.[465] This is a wide exemption and would include both fines from civil proceedings in court, a tribunal, arbitration proceedings and fines under the *DPA 2018*. The data breach led to the loss and exposure of very sensitive personal data belonging possibly to thousands of passengers, the ICO would therefore be very concerned about the damage that this may cause to each data subject. As was discussed above the fines under the *DPA 2018*

[464] For example the class action claims allowed in *Lloyds v Google LLC* [2021] UKSC 50 and *Morrisons Supermarket v Various Claimants* [2018] All ER (D) 89.

[465] See discussion below on the insurability of fines and penalties.

can be quite substantive ranging up to £17,500,000 or up to 4% of the annual world turnover of the preceding financial year, whichever is higher.[466]

The economic or market value of data

4.51. Another exclusion relevant to this scenario is stated in clause 5.1.8 which provides that there shall be no cover for 'the economic or market value of data'. The value of data will vary based on its ability to be used by an organization for economic benefits. There is no set formula for measuring the value of data however there are certain factors which will help to determine its value. These include the exclusivity or uniqueness of the data, its accuracy, potential risks and liabilities from the use of the data, its consistency.[467] If reference should be made to some of the arguments made in *Morrisons v Various Claimants*[468], one of the points discussed was how to assess the extent of damage, by calculating the economic or market value of the data that has been exposed or loss due to the breach. The sale of personal and financial data on the black web for fraudulent activities is a thriving business. Equally lucrative is the practice of selling personal data to advertising companies for marketing campaigns, both of which adds economic value to the data loss. Personal data is also the costliest type of record to be stolen during a data breach. For each personal identifiable record stolen, that would cost an average $180 to CCL. [469] While, the average cost per stolen record in a 2021 was $161 which is an increase from $146 per lost or stolen record in 2020.[470] As it relates to the company data, this places CCL in an extremely fragile position as not only have their reputation been damaged but it is possible that their trade secrets and the customers database which they have taken years to build may now be in the hands of criminals who may sell it to businesses that are competitors of CCL. These businesses / competitors will

[466] UK GDPR 2018, Article 83 (5); DPA 2018, section 157 (5).
[467] PWC, 'Putting a Value on Data' (2019) <https://www.pwc.co.uk/data-analytics/documents/putting-value-on-data.pdf> retrieved 24 September 2020.
[468] [2018] All ER (D) 89.
[469] IBM Security, 'Cost of a Data Breach Report 2021' (IBM Security and Ponemon Institute, July 2021) p. 18.
< https://www.ibm.com/downloads/cas/OJDVQGRY> accessed 24 September 2022.
A record is defined in the IBM Report as 'the information that identifies the natural person (individual) whose information has been lost or stolen in a data breach.' (p. 68).
[470] Ibid 5, 13. The total average cost of a data breach in the transportation industry is 3.75 million in 2021, an increase from 3.58 million in 2020. (p. 15). This number reflects the average costs to CCL following the data breach.

leverage the data and create products that are more personalized to the needs of customers which might eventually lead to the migration of these customers to the rival company. The business opportunities and the commercial advantage which the data lost could bring to CCL is irrecoverable and extremely costly particularly so since the insurers are not willing to indemnify the assured for the economic or market value of the data.

Loss of life, personal injury or illness

4.52. The final exclusion that is of relevance to the assured is 6.3.3 which restricts the extent of collision liabilities by excluding from its ambit liability regarding loss of life, personal injury or illness. There are no reports of a loss of life directly or indirectly caused by the data breach. Instead, passengers and employees are distressed about the loss of control over their personal data. Personal injury is not mentioned in any other clause of the policy so the inference may be that the insurers will indemnify the assured for personal injury sustained onboard the insured vessel provided it is not the result of a collision. This interpretation of the clause would be absurd and against the intention of the insurers who have defined cyber-attack as relating only to physical damage or loss to the vessel or liability of the vessel. Therefore, it would be a futile attempt to argue or expect that the insurers would be willing to indemnify CCL for nonphysical personal injury or damages for the distress experienced by the victims of the data breach. In both circumstances, this would be conflicting to the object and purpose of the policy.

ii. Adequacy of the Marine Cyber Insurance Policy - Data Breach

4.53. The conclusion as it relates to the position of CCL as the assured of SIGCo is that for the losses and liabilities incurred as a result of the data breach, there is no assurance that the insurers will accept the claims. A total rejection of the claim is anticipated primarily because of the absence of what the insurers define as a 'cyber- attack'. Even if the definition was widened to include the events in this scenario, CCL would still encounter challenges because of the exclusions within the policy which unambiguously exempts the insurer from any liability to the third-party victims, for nonphysical damage and their refusal to indemnify the assured for the economic value of data. This leaves CCL in a complicated position where there are numerous gaps in their insurance even

though initially, they may have been convinced they had insurance against cyber risks. The risks and liabilities which arise from the scenario are not the typical risks that will be found in the marine insurance policies. As such, CCL would need to request assistance from his P&I club (provided they are willing to cover those types of loss) or pay the liabilities out of pocket. This is not the most ideal situation for any assured, therefore the coverage provided by SIGCo would not be adequate to cover many of the data breach related losses and liabilities such data recovery costs, notification fees, credit monitoring and public relations consultant fees which do not involve any physical damage. So, while, many assureds in CCL's position may increasingly see the need to purchase marine cyber insurance, the coverage offered is not usually adequate to cover the data protection liability risks to which the business is most susceptible.

b. Cyber / Liability Insurance (CLI)

i. Aviva Insurance Limited - Cyber Insurance Policy[471]

4.54. Imagine that CCL has purchased cyber insurance from Aviva bearing the same clauses as published in their sample policy wording, what would be the implications for CCL considering that the company has just experienced the data breach? It is accepted for these purposes that the incident occurred during the period of the insurance thus there is no contention between the parties as to the existence of a policy at the time of the incident or the date when the incident came to the knowledge of the assured. Having established this very important point, the discussion which follows will consider the terms of the policy to decide whether CCL would have adequate protection against the liabilities incurred as a result of the data breach. Aviva's policy was not written specifically for the marine industry however the focus is on the protection of the assured against data breach. The policy is not divided into numbered clauses, instead each clause will be referred to by the headings used to distinguish it from the other. The main liabilities covered include the following:

[471] Aviva Insurance Ltd, 'Cyber Insurance Policy ' (BCOAG15081 12.2020) <https://www.aviva.co.uk/adviser/documents/view/bcoag15081.pdf> accessed 24 September 2022.

i.i. Data Security breach

4.55. There will be cover for data security breach which includes the cost for specialist consultants whose job is to determine whether there was a genuine data breach and to mitigate an ongoing loss. There is cover for external legal advice and public relations consultants who will advise on how to minimize negative publicity resulting from the data breach. This is important since CCL must ensure that their reputation is not tarnished to the point of unrepairable damage to threaten the existence of the business. Furthermore, if you recall from our discussion above on the UK GDPR / DPA 2018, the controller is required to notify all data victims of a breach which they consider to be serious. The nature of the data exposed, and the number of victims will qualify the incident onboard Santa Maria as a serious breach, consequently, CCL being the controller of the data will be legally required to notify all the victims of the breach. The exorbitant costs[472] which may be associated with such a task is a cause of concern for any business or shipowner, therefore CCL would be pleased to know that Aviva Insurers will absorb the costs of notifying the data subjects and the relevant regulatory body (ICO) of the breach. Credit monitoring services for a period of one year and identity fraud remediation services for data subjects are expenses recoverable from the insurers.

i.ii. Legal liability and Claims compensation

4.56. Additional support is provided under the Data Privacy and Confidential Liability clause. Here the insurer has agreed to cover the legal liability, pay compensation, costs and expenses regarding any claim notified within the period of the insurance or within thirty (30) days of the expiry of the claim. From CCL's perspective, this offers a small degree of security in that they have an extra thirty days to notify the insurers of any breach which occurs during the lifetime of the policy. In other words, their protection under the policy does not end abruptly on the expiration date of the policy. Whereas this is a benefit to the assured, the thirty (30) days after the expiration of the policy is quite short considering the nature of cyber-attacks. The detection of a cyber-attack

[472] The average total costs for the notification aspect of data breaches in 2021 was measured as $0.27 million which accounted for 6% of the average total costs of a data breach ($4.24m global average).
IBM Security, 'Cost of a Data Breach Report 2021' (IBM Security and Ponemon Institute, July 2021), 16 < https://www.ibm.com/security/data-breach> accessed 24 September 2022.

or data loss can take from minutes to years, therefore the assured may be left in a position where knowledge of the data breach, legal liability, expenses or costs do not arise until after the excess 30 days.[473] In such a situation, the assured would have been denied a claim against their insurers because they missed the limitation period. Fortunately, CCL is not in this position since the data breach was identified and immediately reported to the insurers during the policy period. CCL is not required to present the final expenses, costs or legal liability fees to the insurers before or at the 30 days expiration, instead CCL is only expected to give notice of the claim to the insurers.

4.57. Under the data privacy, confidentiality and liability clause, the insurers will cover costs relating to the breach of confidence in respect of the private information or personal data of any individual. Provision is also made for the breach of data protection regulations regardless of the extent of the damage resulting from unauthorized destruction or disclosure or unauthorized access to personal data. There is restricted cover for loss, disclosure or destruction of third party confidential commercial information held under an agreement resulting in financial loss. Such a loss must result from the use of computer equipment by the insured in connection with the business within defined territories[474]. Equipment as defined in the policy includes data storage material such as Alvin's USB flash drive used for processing, communicating and storing electronic data. Is the use of the flash drive by Alvin for personal reasons equivalent to 'use of computer equipment by the insured in connection with the business within the defined territories' as is the requirement under the clause? The definition of insured includes the employees of the CCL however using a USB for personal pleasure should not be accepted as meeting the terms of the clause since Alvin's actions had nothing to do with the business of CCL. He was not instructed to use his USB for any task closely related to his role as a crew member for example to entertain or to provide assistance to guests onboard the vessel therefore it is difficult to imagine that CCL would successfully be covered under this clause of the contract for the actions of Alvin which led to the losses and liabilities incurred in this scenario.

[473] Ibid 21-22. 'The data breach life cycle is the period between first detection of the breach and its containment. In 2021, it took an average of 212 days to identify a breach and an average of 75 days to contain a breach. The total life cycle is 287 days.'

[474] According to the definition section of the policy, defined territories are Great Britain, Northern Ireland, the Channel Islands, the Isle of Man, or offshore installations within the Continental Shelf around such territories.

i.iii. Virus, Hacking & Denial of Service Attack

4.58. Of importance to this claim is the Clause labelled Virus, Hacking & Denial of Service Attack as the insurer contracts that they will cover any cost of reinstating data on a storage device and to locate and remove a detectable virus contained on any computer equipment on the condition that such costs was necessarily and reasonably incurred. The costs incurred in either situation should be caused by or resulting from a virus or similar mechanism, hacking or a denial of service attack directed against CCL or any outsourced service provider. The requirement that the costs be necessarily and reasonably incurred was not defined in the policy, however what is necessarily and reasonably incurred is fact dependent and will vary based on the circumstances of each case. The procedures undertaken must be of such a nature that they are essential and proportionate to the curtailment of the breach. Through the Network Security Liability clause, the assured will be indemnified for the negligent transmission of a virus or failure to prevent unauthorized access to the data. CCL would be very pleased with this term of the cover since the transmission of the virus onboard was partially due to their negligence in failing to institute procedures that would have prevented unauthorized access to the data. Such a clause appears to encourage moral hazard, but it may be a balancing exercise in that parties understand that errors and mistakes may occur without the deliberate defiance of security guidelines or recklessness, the latter behaviour would not be covered by the insurers.[475]

i.iv. Exclusions and Gaps in the cover

4.59. While there is a greater sense of security for data related losses under this insurance policy, there are exclusions which will expose the Assured to many uninsured liabilities thus underlining the gaps in the assured's insurance policy. There is no cover for losses incurred due to the theft of trade secrets, license fee or royalty relating to intellectual property. With that said, if the company data which has been stolen fits any of these descriptions, CCL would be without insurance. Essentially, this means that CCL needs to find alternative protection against such loss. Trade

[475] Among the exceptions to the Network Security Liability Clause is exception (6) – 'any Virus or Similar Mechanism created or knowingly transmitted by the Insured other any Virus or Similar Mechanism created or knowingly transmitted by an Employee who is not a director or partner acting intentionally outside their scope of authority'.

secrets would include customers data, CCL specialized marketing and entertainment techniques and processes. Equally important is the contractual arrangements that may exist between CCL and other cruise operators, travel agents and or the Tourism Board of different states which help to create a competitive advantage for CCL with access to an ongoing stream of customers and the countries of interest that is part of their tour package. CCL would also have contractual arrangements with entertainers, food suppliers and a valuable database of custom documents, vessel certificates which cumulatively makes it easier for CCL to provide their service and maintain their reputation as a preferred brand within the market. This is a gap in the policy with which no assured will be completely contented since they have invested years and time in building their data and honing their trade secrets to make their mark in the industry.

i.v. Compensation to employees

4.60. Another exception is that the insurers will not provide cover for any proceeding or claims relating to compensation for any employee. This clause is problematic for CCL who anticipates an influx of claims from employees. Fortunately, there is a proviso which states that the exclusion does not relate to claims for breach of confidence of any employee or the misuse of employees' private data.

i.vi. No cover for liability arising from personal injury

4.61. Furthermore, another relevant exclusion is the lack of cover for 'liability arising out of personal injury or physical loss, destruction or damage to property'' Personal injury shall include mental anguish, emotional distress, and discrimination, which is a more extensive meaning than that found in most insurance policies when reference is made to personal injury.[476] The term takes on the recognized definition given to personal injury in tort law. The more extensive meaning is a good for CCL and other data breach subjects as mental anguish and emotional distress are the

[476] Among the exceptions to the Data Privacy and Confidential Liability Clause is exception (8) – 'liability arising out of Personal Injury or physical loss, destruction or damage to Property. For the purposes of the above covers Personal Injury shall also include mental anguish, emotional distress and discrimination. However, this exclusion shall not apply in respect of claims for mental anguish or emotional distress arising from defamation or breach of confidence in respect of any individual or misuse of any individual's private information or Personal Data or breach of Data Protection Regulations.'

typical damage that will result from data or privacy breach. CCL benefits from this clause since the exclusion does not apply to claims for mental anguish or emotional distress arising from a breach of confidence or misuse of an individual's private information, personal data or any breach of the Data Protection Regulations.

ii. Beazley Breach Response Policy

ii.i. The Introductory Clause

4.62. Coverage is provided on a claims made and reported basis and applies only to claims first made against the insured during the policy period or the optional extension period.[477] This means that a claim must be made both against the insured and reported to the insurer during the policy period for coverage to apply. This is not the most ideal for the insured since claims made against him close to the expiration of the policy might not get reported before the policy expires, however this unfavourable position can be eliminated if the assured agrees to an optional extension period in applicable situations. Even where the assured agreed to an optional extension, there is no blanket application of the extension to all the clauses of the contract, therefore the assured must recognize that some liabilities will be covered while others will not. It is important that it is made clear to the assured the clauses to which the optional extension is applicable.

ii.ii. Breach Response Services

4.63. Under the insurance agreement, the insurers are prepared to provide breach response services to CCL, because of an actual or reasonably suspected data or security breach that the assured first discovers during the period of the insurance. In the scenario with Alvin, there is no doubt as to the existence of a security breach as the system failed to prevent the virus from infecting the computer systems onboard Santa Maria and its offshore facility. Yet, it is reassuring for any assured to be confident that their insurer will provide breach response services for a reasonably suspected breach. This means that the clause does not operate on an indemnity basis, a principle deeply entrenched in marine insurance whereby 'the underwriter undertakes to indemnify the

[477] Beazley, 'Beazley Breach Response: Introductory Clause' (nd)
< https://policies.dppl.com/policy.php?policy_number=BBR-5A8ED7A3-8OEF> accessed 24 September 2022.

assured in the manner and to the extent thereby agreed against marine losses ' in other words, if there is no loss or damage to an insured risk, the insurer will not pay.[478] The problem here is what will qualify as a suspected breach, reasonable indicators of a suspected breach and the accepted response procedures for such suspicion. These are details which the assured must discuss and agree with their underwriter during the negotiating period of the policy. Essentially, including a definition for suspicion would remove some of the ambiguity surrounding this clause especially for small to medium sized businesses who may lack the technical expertise to properly assess their vulnerabilities.

> A breach response service means the fees and costs in response to an actual or reasonably suspected data or security breach[479];
>
> 1. for an attorney to provide necessary legal advice to **CCL** to evaluate its obligations pursuant to ***DPA, GDPR 2018*** or any other statute or regulation or merchant services agreement and in connection with providing the breach responses services below;
> 2. for a computer security expert to determine the existence, cause and scope of an actual or reasonably suspected data breach, and where such breach is in progress to contain it;
> 3. for a PCI Forensic Investigator to investigate the existence and extent of an actual or reasonably suspected Data Breach involving payment card data and for a Qualified Security Assessor to certify and assist in attesting to the Insured Organisation's PCI compliance, as required by a Merchant Services Agreement.
> 4. to notify those individuals whose personally identifiable information was potentially impacted by a data breach exceeding the notified individuals threshold;
> 5. to provide a call centre to respond to inquiries about a data breach that exceeds the notified individuals threshold;
> 6. to provide a credit monitoring, identity monitoring or other solution described in the Information Packet to individuals whose personally identifiable information was potentially impacted by a data breach exceeding the notified individuals threshold; and
> 7. public relations and crisis management costs directly related to mitigating harm to the insured organization which are approved in advance by the Underwriters in their discretion.

The costs allocated for breach response services excludes any internal salary or overhead expenses CCL will pay to facilitate recovery during and after an actual or suspected breach. This is a

[478] MIA 1906, s. 1.

[479] Beazley, 'Beazley Breach Response: definition breach response services' (nd) < https://policies.dppl.com/policy.php?policy_number=BBR-5A8ED7A3-8OEF> accessed 24 September 2022.

significant setback for the business as CCL will need to have staff working overtime to mitigate and remedy the breach in a timely manner. Some staff especially those in more senior roles will be required to assist expert contractors with the investigation process and may be asked to prepare reports to regulatory bodies such as the ICO. Extra working hours means that utility bills will also increase along with all other expenses which would be invested in facilitating the recovery process. To reiterate, this significantly affects **CCL** as money is allocated towards these costs for which they have not budgeted and during a period when they are already in a precarious financial position.

ii.iii. Breach Response Limits of Liability

4.64. The aggregate limit of liability is the underwriters combined total limit of liability for all losses other than those falling under the breach response services. This means that the costs for breach response coverage will be in addition to the aggregate limit of liability. Separating the breach response limits from the aggregate policy is a good approach that will enhance and protect the interest of the assured since the breach response services could quickly exhaust the aggregate limit of the policy.[480] In this way, CCL need not be too worried about using too much of the insurance money on the breach response. It is important that the most effective breach response procedures and services are implemented and made available to the assured without financial constraints as this is the only way that the risk will be controlled, and the losses curtailed to a degree that may prevent the downfall of the business.

ii.iv. Notification Limits

4.65. Among services offered under breach response is the notification to data subjects whose personal information has been exposed or is suspected of being unlawfully exposed due to the data or security breach. There is a notification threshold which is the 'maximum total number of individuals to whom notification, call centre and credit identity monitoring services will be

[480] The average total costs for the notification aspect of data breaches in 2021 was measured as $0.27 million which accounted for 6% of the average total costs of a data breach ($4.24m global average).
IBM Security, 'Cost of a Data Breach Report 2021' (IBM Security and Ponemon Institute, July 2021), 16 < https://www.ibm.com/security/data-breach> accessed 24 September 2022.

provided or attempted for all incidents or series of incidents giving rise to an obligation to provide breach response services.' The maximum number of individuals to whom notification will be provided is 5 million, when exceeded the insurer has no contractual obligation to indemnify the assured to notify or provide monitoring services to anyone above the threshold limit. For small and medium sized business, the 5 million threshold may be enough as not many businesses will have that many customers information stored in their database. However, for a passenger vessel like Santa Maria, a limit of 5 million individuals could possibly be just a cross-section of the passenger details or personal information which they have stored.[481] The first 5 million data subjects to be notified and to whom credit monitoring services is to be provided will be paid for by the insurers. This amount is in addition to the aggregate limit of the policy which is USD$15 million. CCL would be responsible for notifying, providing call centre services, identity and credit monitoring to all the individuals above the threshold.

4.66. In the event that the number of individuals whose data have been stolen from CCL exceeds 5 million, this is not the end of the road for CCL as the insurers have made available an additional breach response limit which operates in two circumstances, either where the notified individuals limit has been exceeded or the limits for other breach response services have also been exceeded. In either case, the insurers will cover the costs, fees and expenses incurred to provide such breach response services up to the policy aggregate limit of liability. The additional breach limit forms part of and is not in addition to the policy aggregate limit of liability. The way this works is that the breach response services are divided into two towers with separate limits. There is tower 1 which covers computer expert services, PCI forensic investigator, legal services and crisis management and public relations with a limit of up to USD$2.5 million. The second tower comprises of the notification and call centre services, credit and identity monitoring with a limit of up to 5 million individuals. The remaining services under the policy will fall under the third

[481] An example of the number of passengers that travel on passenger vessel per year Carnival Corporation & plc is the largest leisure travel company and parent company of Carnival Cruise Lines which has been the victim of several data 2020 and 2021. The company 'employs over 150, 000 people from nearly 150 countries and hosts nearly 13 million guests annually with more than 325.000 people sailing aboard Carnival Corp vessels each day.'
Carnival Corporation & plc, 'Corporate Information' (n.d) < https://www.carnivalcorp.com/corporate-information> accessed 24 September 2022.

tower to include third party information security and privacy coverage, regulatory defence and penalties, website and offline media liability, PCI fines, penalties and assessments and first party coverage totalling an aggregate of USD$15 million.[482] Where the limits in either tower 1 or 2 are exhausted due to a breach, cover will be provided for the additional breach response services through the limit available in the third tower. The amount that will be contributed to the additional breach response services is the unspent money remaining after the costs for first and third party loss that have been subtracted from the aggregate policy limit of USD$15 million. This is beneficial to the assured only when there is a surplus in the third tower after first and third party losses have been covered.[483] The issue is complicated by the fact that third tower includes cover for the costs of regulatory defence and penalties such as fines under the **UK GDPR / DPA 2018**. If the ICO should conclude that **CCL** has seriously breached many of the principles of the DPA and large numbers of personal data have been compromised or lost, it is very likely that the fine imposed by the ICO would exceed the $15 million which the insurers are prepared to pay especially when comparison is made with fines and penalties imposed by the ICO in the case studies discussed earlier. Even so, there is uncertainty as to whether those penalties are insurable. The policy itself simply states that the' insurability of penalties will be in accordance with the law in the applicable venue that most favours coverage for such penalties.' Therefore, even though the policy explicitly provides that the insurer will pay for regulatory defence and penalties costs, this service will be retracted in jurisdictions where regulatory fines and penalties are non-insurable and uncertainty looms in other jurisdictions where the position is not clear.

ii.v. Data recovery costs

4.67. The insuring agreement also includes the commitment by the insurer to indemnify the assured for data recovery costs as a direct result of a data breach which the insured first discovers during the policy period. The data recovery costs 'means the reasonable and necessary costs incurred by the insured organization to regain access to, replace, or restore data, or if data cannot

[482] Beazley, 'Beazley Breach Response (BBR) in Cyber & Tech: Understanding the coverage' (n.d) <https://www.beazley.com/usa/cyber_and_executive_risk/cyber_and_tech/beazley_breach_response/understanding_the_coverage.html> accessed 24 September 2022.

[483] BBR Boost Coverage Animation (n.d) <https://player.vimeo.com/video/265762112> accessed 24 September 2022.

reasonably be accessed, replaced or restored, then the reasonable and necessary costs incurred by the insured organization to reach this determination.' The costs will not include the monetary value of profits, royalties, or lost market share related to data, including but not limited to trade secrets or other proprietary information or any amount pertaining to the value of data; legal costs or legal expenses; loss arising out of any liability to any third party or cyber extortion loss.

ii.vi. Other covered Liabilities

4.68. Liabilities covered that are applicable to this scenario include the following clauses:

Data & Network Liability

To pay Damages and Claims Expenses, which the Insured is legally obligated to pay because of any Claim first made against the Insured during the Policy Period for:

1. A Data Breach;
2. …

> **Regulatory Defence & Penalties**
>
> To pay **Penalties** and **Claims Expenses**, which the **Insured** is legally obligated to pay because of a **Regulatory Proceeding** first made against any **insured** during the **Policy Period** for a **Data Breach** or a **Security Breach.**
>
> **Payment Card Liabilities & Costs**
>
> To indemnify the **insured organization** for **PCI fines and expenses and costs** which it is legally obligated to pay because of a **claim** first made against any **insured** during the **policy period**.

Credit and debit card payments are one of the many ways in which cyber criminals involved in this data breach will benefit. A cruise line such as this, operated by CCL will be the controller of millions of passenger credit and debit card details. These passengers would have booked their trip through the CCL's booking website while others could have used their cards to pay for various services while onboard the vessel. As a result of the potentially high gains from this venture, any successful access to the data held by these cruise companies will be a lucrative target for those responsible for this security and data breach. These fines and expenses, with the prior approval of

the underwriters will cover the reasonable and necessary legal costs and expenses incurred by CCL to appeal or negotiate an assessment of the monetary amount said to be under a merchant services agreement due to the breach.

ii.vii. Exclusions

Liabilities arising out of bodily injury or property damage

4.69. The policy will not apply to any loss arising out of bodily injury or property damage, thus excluding any physical injury including mental anguish or emotional distress resulting from such physical injury, sickness, disease or physical injury to tangible property[484]. The clause excludes mental anguish or emotional distress resulting from physical injury, sickness, disease or death. This implies that if mental anguish or emotional distress results from non-physical injury such a data breach onboard Santa Maria, it is likely that the assured will be protected against such risks. The correctness of this approach might be challenged by insurers but until the clause is made clear, there is room for alternative interpretation to the advantage of the assured.

iii. Adequacy of a Cyber Liability Insurance in response to the Data breach

4.70. Generally, the insurance coverage offered by cyber liability insurers provide a more comprehensive protection for the liabilities incurred than that which will be provided under a policy written specifically for hull and machinery insurance with a cyber endorsement. To the advantage of the assured most of the liabilities which will arise due to a data breach will be covered including the recognition of mental anguish and emotional distress due to the breach of the UK GDPR / DPA 2018. The insurers are willing to pay for legal and consultants fees relating to the breach, the latter to counter and control any negative publicity. These policies have extensive breach response clauses that includes credit monitoring services, notification fees and most of the necessary costs incurred when a data breach occurs. The Beazley Breach Response for example has high and flexible limits of liability giving the assured the opportunity to take the most

[484] Beazley, 'Beazley Breach Response: Exclusions Bodily Injury or Property Damage' (nd) < https://policies.dppl.com/policy.php?policy_number=BBR-5A8ED7A3-8OEF#pagenav-ex-1F> accessed 18 September 2022.

advantage of their insurance coverage through the extensions and towers of liability. The exclusion on physical injury which includes mental distress is not very clear however the victim of a data breach does not need to establish a financial loss or mental distress to be able to claim damages. In the end, the assured CCL would gain the most from his cyber insurance policy following the data breach in this scenario. The following summary points will give a clear view on the adequacy / inadequacy of cyber and traditional marine insurance to a data breach.

IV. Chapter Summary

Nature of the risks

- Passenger vessels are lucrative targets for cyber criminals as they are personal data tanks with an online value of millions on the dark web as such data breach is a real risk to the maritime sector with potential liability being extremely high for shipowners / carriers.

- It is unlikely that a data breach will be considered a shipping incident or of the same genus as act named and that can be pursed against the owners / charterers under the Athens Convention and amended Protocol 2002. The Convention was not created to regulate every kind of neglect or harm onboard the vessel.

- CCL will not be vicariously liable for losses arising from a data breach, caused by a Alvin who uses his personal device to connect to the company network and in the process inadvertently infected the computer systems as his actions were not closely connected to his employment nor was he acting in the course of his employment. The inadvertence of the employee / crew member is irrelevant in establishing close connection.

Regulatory Measures

- Each passenger or crew whose data protection rights has been breached and as a result has experienced emotional distress may be compensated in damages without the need to establish pecuniary or physical loss. The data subject has the option to pursue a claim against the data

controller, CCL in tort of misuse of private information and claims to the ICO under the UK GDPR / DPA 2018.

- The position as to the insurability of fines under the UK GDPR / DPA 2018 is unclear so CCL must be prepared to cover the fees arising therefrom in the event there is a declaration that such fines are uninsurable. However, that will depend on the location of the data subjects and the jurisdiction in which the matter will be heard. The rules vary even across the EU member states. Despite the differences, there is a general consensus that data protection breaches that are criminal or quasi-criminal will not be insurable. Administrative fines may or may not be insurable depending on the degree of negligence, moral turpitude, and public policy considerations. It is unlikely that UK GDPR / DPA 2018 fines will be insurable.

- The violation of cyber security safety regulations should not be declared 'illegal' as they are not of such moral turpitude to deny a ship owner or any other assured his right to insurance. The breach of marine and cyber risks safety regulations should be an issue relating to seaworthiness rather than an issue of illegality.

Traditional Marine Policies

- Traditional marine insurance policies do not provide any cover against liabilities or losses incurred as a result of a data breach due to the commonly used CL.380 and the newer LMA5402: Marine Cyber Exclusion which excludes loss from non-malicious, non-intentional events such as the failure, error or malfunction of any computer system, software program or code. Another reason is that traditional marine insurance policies focus on physical loss or damage to tangible property such vessel, cargo but not electronic data.

- For some assureds, particularly SME, the most affordable solution to their gaps in insurance coverage is to purchase or make a request for a cyber endorsement to their traditional marine insurance policies. Recent endorsement clauses include LMA5403 which would indemnify CCL for computer related losses provided they were not used or operated as a means for inflicting harm. The problem with endorsement clauses is that new perils for example a data

breach will not be covered by insurers as the endorsement is subject to the terms, conditions and exclusions of the original policy.

Cyber Liability Insurance

- Depending on the language of the policy, some cyber insurance policies designed specifically for the marine market will not recognize a data breach as a cyber-attack, so CCL as the owner / carrier will not be indemnified for any loss or liability arising from a cyber-attack / data breach which causes non-physical damage. CCL would need to have had in place a cyber insurance not necessarily designed for the marine sector which recognises and will compensate the assured for loss from a data breach and its associated liabilities.

- Cyber insurance covers mostly nonphysical damages for example data security breach which includes the cost for specialist consultant, ongoing loss, external legal advice, and public relations consultants who will advise on how to minimize negative publicity resulting from the data breach. There is also coverage for costs of notifying the data subjects and the relevant regulatory body for example ICO. In addition, there is credit monitoring services and identity fraud remediation services for data subjects.

- Most will exclude costs for the value of the data lost and will not pay for trade secrets or company documents and information. The focus is on the personal data of the natural individual. CCL would need to seek the costs to replace company information from other insurers.

- Some insurers are also not prepared to cover the costs for any repairs, assembling, replacement of any electronic data, computer software or hardware. Such wording would not be in the best interest of CCL or any assured who has experienced a breach and have had damage to software and other computer or electronic equipment. Betterment is often not allowed but there are exceptions in some policies where it is impossible to obtain the old model or its cheaper to buy or repair with a newer improved version of software etc.

- Most of the cyber policies exclude claims for personal injury and the Beazley policy was keen to clarify that personal injury also include mental distress. There are exceptions where mental anguish or emotional distress from a data breach will be exempted from the personal injury exclusion. CCL might need to request the assistance of their P&I club to address this cost. Though admittedly not a typical P&I risks, data protection liabilities have not been exempted from P&I cover but will depend on nature of the breach and the discretion of the Board.

- Cyber insurance policies include extensive and a diverse list of exclusions denying protection against losses and perils many assured would expect to be covered. In addition to those already mentioned, the more commonly found exclusions include but are not limited to the costs of updating or upgrading the assured vessel, the cost of repairing, recreating, gathering or assembling an electronic data or computer software or the repair or replacement of any parts or components of any computer hardware, third party liability such as lawsuits, claims or demands by an employee, officer, director or partner of the assured, the economic or market value of data, punitive or exemplary damages, fines or penalties of any nature, loss of life, personal injury or illness inter alia. The exclusion of third-party claims is often found in cyber insurance policies. They deny assureds of the right to be indemnified or to be subrogated by insurers in individual or class action claims brought against the assured by employees, officers, directors, or partners.

- Generally, cyber liability insurance provides a more comprehensive protection for liabilities related to a data breach than the coverage provided under a policy written specifically for hull and machinery insurance or any traditional marine policy with a cyber endorsement.

Way Forward

- Shipowners must impose security measures to prevent crew access to the parent network and from connecting their personal devices directly to the vessel. To protect the ship and offshore networks, the best practice is to segregate crew and entertainment networks from the other ship

networks and ensure proper procedures are in place for the safe use of removeable media in accordance with industry and IMO guidelines.

- There is no formal statement from the ICO or other legal entity in the UK on whether fines and penalties imposed under the DPA and UK GDPR are insurable. This is in stark contrast to the position held by the Financial Conduct Authority. In the absence of a statement from the ICO clarifying this issue, the London market should publish a unified stance on the insurability of fines, so assureds are certain about what they are purchasing when buying insurance against cyber risks and data breach. It may be worth having a two (2) limb approach by allowing insurance of fines that were not the result of gross negligence, criminal or malicious acts of the assured or his agents while fines caused by other means are uninsurable. Cyber insurance policies that exclude fines or penalties do not adequately protect assureds from many of the risks unique to data breach such as notification fees, credit monitoring and public relations consultant fees and the very high that may arise from civil proceedings in court, arbitration matters and fines under the DPA and GDPR 2018.

Scenario 4: Port Lockdown!

Denial of service attack resulting in business interruption and reputational Harm

The ports of Liverpool experienced a denial of service (DOS) attack where all systems have been disabled and encrypted. This was made possible when cybercriminals transmit bugs onto the port networks which was operating on an outdated Windows 7 system which had no support for patches since 14th January 2020. The hackers refused to free the system until a ransom amount of £10 million is paid to them in bitcoin. This prevented operation in several other ports and affected the supply chain on which many stakeholders depended as the port community system was also compromised. This was the 2nd cyber-attack on the port's network in two (2) months. All efforts to negotiate with the hackers were unsuccessful. The port authorities decided not to pay the ransom as such the port remained closed for another fifteen (15) days before operations were restored at full capacity. The DOS attack meant that there was significant business interruption claims along with reputational damages.

Content **Pages**

I. Port Lockdown!

A. Why target Ports?

5.1. The UK has designated some of its ports and port facilities as critical national infrastructure both for their geopolitical and economic significance.[485] Ports can be collectively viewed as the lifeline of the maritime sector; they function as the main point of transit for various goods on which the economy and sustainability of the nations within the UK depend. Other services provided by ports include vessel berthing, vessel loading and unloading, temporary storage and staying, distribution and transfer, security and safety and general support services. As the world becomes more digitized and greater dependence is placed on Information Technology (IT) and Operational Technology (OT) systems[486], some port authorities have found it necessary to begin to transform ports into smart ports. This means that many systems and processes within the port will rely on digital technology and in some instances automated systems to enhance connectivity, visibility and control, improve services along the supply chain and to comply with internationally recognised cyber security standards. Additionally, storage of data is being moved to the cloud and robots and artificial intelligence are fast becoming the new norm in a bid to maintain or gain a competitive edge in a technologically driven market. On the other hand, there are ports which have not invested much in the transition to 'smart ports', nevertheless they are still susceptible to many of the cyber risks to which smart ports are most vulnerable.

[485] The Network and Information Systems Regulations 2018 (NIS 2018), Schedule 2 paragraph 5, explains the threshold requirements which apply to essential services in the water transport sector. The essential services mirror the UK 13 Critical National Infrastructure sectors which includes both Transport and Water sectors. "Critical Infrastructure is defined as those critical elements of infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life." National Cyber Security Centre, 'CNI Hub' (n.d) <https://www.ncsc.gov.uk/section/private-sector-cni/cni> accessed 15 September 2022.

[486] Information technology systems focus on the use of data as information. Operational technology systems focus on the use of data to control or monitor physical processes.
IMO, 'Guidelines on Maritime Cyber Risk Management' (MSC-FAL.1/Cir.3, 5 July 2017) para 2.1.2
< MSC-FAL.1-Circ.3 - Guidelines On Maritime Cyber Risk Management (Secretariat).pdf (imo.org)> accessed 15 September 2022.

5.2. While the technological developments are laudable, ports are not immune and continue to be targets of cyber criminals. In fact the maritime sector has seen a 900% increase in cyber-attacks in three (3) years.[487] Robert Rizika, Naval Domes Head of North American Operations, while speaking at the 2020 Port Security Seminar & Expo virtual conference explained 'that in 2017 there were 50 major operational technological hacks reported, 120 in 2018, 310 in 2019 and it is expected that 2020 will end with more than 500 reports of major attacks, bearing in mind that there will be many more incidents that have not been reported for the same periods.'[488] The cybersecurity incidents at the Port of Antwerp[489], the ransomware attacks in the Port of Barcelona and San Diego[490], Shahid Rajaee port terminal in Iran[491] the attempted attack at the Port of Houston[492] and the cyber-attacks on the Port Of Los Angeles since the pandemic[493] are notorious and they demonstrate the geographic scale of the risks.

5.3. Cyber-attacks threaten the economic and physical stability of ports leaving the port authorities exposed to significant liability claims which they may be unable to afford. Equally detrimental is the crippling effect on the global economy whereas in this scenario, a cyber-attack

---

[487] Compass Handbooks 'Maritime cyber attacks increase by 900% in three years' (July 20, 2020) <https://uk-ports.org/maritime-cyber-attacks-increase-by-900-in-three-years/> accessed 16 September,2022.

[488] Ibid.

[489]Port of Antwerp, 'Port of Antwerp steps up fight against cybercrime' (23 October 2013) <https://www.portofantwerp.com/en/news/port-antwerp-steps-fight-against-cybercrime> accessed 31 December 2021; Tom Bateman, 'Police warning after drug traffickers; cyber-attack' *BBC News* (London, 16 October 2013). <https://www.bbc.co.uk/news/world-europe-24539417> accessed 16 September 2022; DW, 'Belgium investigates cyberattack on energy companies' *Deutsche Welle* (Germany, 03 February 2022) <https://www.dw.com/en/belgium-investigates-cyberattack-on-energy-companies/a-60651892> accessed 16 September 2022.

[490] IMAREST, "Ports of Barcelona and San Diego hit by cyber attacks' (28 September 2018) <https://www.imarest.org/themarineprofessional/4473-ports-of-barcelona-and-san-diego-hit-by-cyber-attacks> accessed 16 September 2022.

[491] Mission Secure, 'Maritime Security Incidents: Disruptive Cyber-attack Cripples Port Facility' (5 August 2020 updated 14 December 2020) < https://www.missionsecure.com/blog/disruptive-cyber-attack-cripples-port-facility> accessed 16 September 2022; Joby Warrick and Ellen Nakashima, 'Officials: Israel linked to a disruptive cyberattack on Iranian port facility' *The Washington Post* (Washington DC, 18 May 2020) <https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html> accessed 16 September 2022.

[492] Olafimihan Oshin, ' Major US port target of attempted cyber attack' *The Hill* (Houston, 23 September 2021) < https://thehill.com/homenews/state-watch/573749-major-us-port-target-of-attempted-cyber-attack > accessed 16 September 2022.

[493] Sam Fenwick, 'Cyber-attacks on Port of Los Angeles have doubled since pandemic' *BBC News* (Los Angeles, 22 July 2022) < https://www.bbc.co.uk/news/business-62260272> accessed 16 September 2022.

halts operations at several ports. Lloyds estimates that the damage to the world economy from a cyber-attack on fifteen (15) Asian ports may range between $40.8 billion in the least severe scenario (6 ports affected), to $55.9 million (9 ports are affected) to $109.8 billion in the most severe scenario.[494] Business Interruption and contingent business interruption coverages are the main insured losses with 63% of the total losses for the least severe scenario and 60% for the most severe scenario. Also, in the most severe scenario, port operators will carry 50% of the insured loss.[495] Accordingly, it is expected that after a cyber-attack on a port or port facility, the port operators will depend on their insurers to respond to various type of claims including business interruption and reputation losses.

5.4. Against this background, I will analyse whether the traditional business interruption policies will respond to liability and losses caused directly or indirectly from a cyber-attack. Following this analysis, I will examine some of the available cyber business interruption policies to determine whether the coverage provided against cyber risks is adequate to protect the assured's interest. For the purposes of this discussion, it will be assumed that the ship owners and the port operators in this scenario have purchased the traditional marine insurance covers for their businesses and that causation has been established. It is therefore accepted that the disruption to the operations of the port of Liverpool was caused by the DOS attack, however the exact source of the attack is unknown so too is the response of the insurers.

5.5. There are several international and domestic instruments which address port security and more specifically guidelines detailing best practices and recommended procedures to prevent, detect, assess and respond to cyber threats at ports and port facilities.[496] To be compliant with these cybersecurity guidelines, ports are encouraged among other things, to develop a port facility

[494] Lloyd's of London, Cambridge Centre for Risk Studies and Nanyang Technological University, 'Shen attack: Cyber risk in Asia Pacific ports' (2019) 55. <https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/shen-attack-cyber-risk-in-asia-pacific-ports> accessed 17 September 2022. There were 3 scenario variants in the report reflecting low probability to high impact situations. The S1 variant affects ports in Japan, Malaysia, and Singapore. The S2 variant adds the Republic of Korea to S1 countries and the X1 variant adds China to S1 and S2 variants for a total of 15 ports affected.

[495] Ibid.

[496] The analysis throughout this research focuses on the insurance aspect of cyber risks and not on the regulatory side of cyber risks. Therefore, the details of these Regulations, international instruments and Guidelines are beyond the scope of this research.

security assessment, a port security plan and train personnel to identify and respond to cyber risks and vulnerabilities in systems.

B. The nature of business interruption insurance

5.6. Business interruption insurance covers loss of profits and damages to physical assets but does not usually compensate for virtual assets such as the damage to software and data. This is irrespective of the commercial value of the latter as compared to the physical assets.[497] Conversely for cyber risk business interruption (CRBI), the assured is not required to establish that there was physical damage to property nor is there the requirement for the assured to have in place a separate property damage insurance policy (material damage proviso); damage to software and data or interruption to the company network is sufficient even though more difficult to prove than physical damage.

a. Business Interruption (BI) and how is it calculated?

5.7. Business interruption insurance is created to indemnify the assured for specified losses such as loss of profits that would have been earned but for the interruption caused to the business from an insured peril.[498] The difficulty is calculating what the turnover of the insured would have been and what percentage would have been profit.[499] The growing practice is for the parties to agree to a liquidated sum per day, a technique believed to eliminate the uncertainties associated with the proof and calculation of turnovers.[500] Another system of calculation is based on the 'gross earnings' or 'business income' approach which is more popularly used in the US market while the loss of turnover / loss of profit (gross profit) is the preferred method of calculation in the UK.[501]

---

[497] Gary Hibbert and Alan Cook , 'The rise of cyber liability insurance' in Babak Akhgar, Andrew Staniforth and Francesca Bosco (eds), *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Elsevier Science &Technology Books, 2014) p. 222. <https://ebookcentral.proquest.com/lib/swansea-ebooks/detail.action?docID=1744499 > accessed 18 September 2022.

[498] Ozlem Gurses, *The Insurance of Commercial Risks* (5th edn, Sweet & Maxwell 2016) para 15-001.

[499] Andrew McGhee, *The Modern Law of Insurance* (4th edn, Lexis Nexis 2018), para 50.15.

[500] Ibid.

[501] A detailed explanation of the distinctions between UK and US Approaches to Business Interruption Insurance is provided in - CILA & Insurance Institute of London, 'Business Interruption Policy Wordings - Challenges Highlighted by Claims Experience' (Research Study group 265, April 2019) Appendix 1: Key Differences Between UK and US

5.8. Under a UK policy, the insurer agrees to indemnify the assured for the turnover lost by paying the percentage which the gross profit insured contributed to the turnover in the previous financial year before the occurrence of the insured peril that caused the business interruption, taking into consideration business trends.[502] For policies in the UK, the insurer will pay for loss suffered during the repair or rebuilding period.[503] This is in addition to those continuing losses which are a consequence of the damage provided the maximum indemnity period has not expired.[504] The gross profit calculation for business interruption is written on 'the difference basis' which is turnover minus variable charges.[505] Since only the variable costs is subtracted from the turnover, it means cover is provided for wages, net profit and overheads.[506] However, the 'difference basis' approach is not without its limitations given that there is a potential for underinsurance particularly where 'businesses record direct labour as part of the cost of sales which ultimately means there is a reduced accounting profit'.[507] In addition to the net turnover, gross profit must also include the expenditure incurred to minimize the effect of the interruption on the turnover of the business.[508] In the shipping industry, where carriage cost is fixed by contract, this should be treated as a non-variable charge which should be insured.

5.9. The US gross earning or business income approach indemnifies the assured for the period of restoration of the property after damage, however subsequent losses after the repair are not covered by the insurers. Business income is the 'net income that would have been earned plus the

---

Approaches to Business Interruption Insurance <https://www.cila.co.uk/cila/downloads/sig-downloads/business-interruptions/files-9/13-bi-policy-wordings/file> accessed 18 September 2022.

[502] Damian Glynn and Toby Rogers, *Riley on Business Interruption Insurance* (11th edn, Sweet & Maxwell 2021) para 1.10.

[503] CILA & Insurance Institute of London (n 501) para 4.3.2.

[504] ibid

[505] Gross profit in insurance takes on a different meaning from that used in accounting therefore the assured must ensure that he has adequate protection for his business. So, while gross profit may include wages, it does not necessarily include discounts and agents commission, commonly found in accounts profit and loss calculations. Harry Roberts, *Riley on Business Interruption Insurance* (10th edn, Sweet & Maxwell 2016) para 1.4.

[506] This feature distinguishes the difference basis from the net profit approach (additions basis) because in the latter, there is no cover for wages so the assured would need to purchase separate insurance for wages. "The Additions basis of calculation is rarely used in the UK but used elsewhere" for example in the USA (my emphasis added). Glynn and Rogers (n 502) paras 1.10, 1.14 and Appendix E – Example U.K. Business Interruption ("Additions" Basis) Specification – "Gross Profit" Wording – Sum Insured Basis.

[507] Glynn and Rogers (n 502) para 1.14.

[508] Roberts (n 505) para 1.8.

continuing normal operating expenses incurred including payroll'.[509] The focus under the US business interruption forms is reinstatement of the business and indemnifying the assured for the actual loss directly caused by the interruption to the business which is the point at which the coverage begins to respond. There is no predetermined maximum indemnity period. The repairs must be completed within a reasonable time as the insurer will only pay for 'such time as would be required with the exercise of due diligence and dispatch' to complete the repairs.[510] Consequently, while the insurer will cover the actual loss suffered until the damage to the business is repaired, once this is completed the business interruption cover ends even if the business continues to suffer loss.

5.10. Unlike the 'actual loss due to suspension of your operations language written in the US forms, the causative language used in the U.K. form is 'in consequence of'; so that insurers will pay for losses in consequence of the insured damage to the property thereby offering wider protection to the assured. The opening paragraph of The Standard U.K. "All Risks" Policy Form (Business Interruption)[511] illustrates the causal connection required before an indemnity is to be paid for the BI. The paragraph provides:

> The Insurer agrees (subject to the terms, definitions, exclusions and conditions of this policy) that if after payment of the first premium any building or other property used by the Insured at the Premises for the purpose of the Business be accidentally lost destroyed or damaged during the period of insurance (or any subsequent period for which the Insurer accepts a renewal premium) **and in consequence** the business carried on by the Insured at the Premises be interrupted or interfered with then the Insurer will pay to the Insured in respect of each item in the Schedule the amount of loss resulting from such interruption or interference provided that … (emphasis added)

The definitions section of the same policy specifies that insurers will indemnify assureds for "CONSEQUENTIAL LOSS" "which shall mean loss resulting from the interruption of or interference with the business … **in consequence** of loss or destruction of or damage to the property used by the assured at the premises for the purpose of the business."[512]

[509] CILA & Insurance Institute of London (n 501) page 66.
[510] ibid pages 63 – 69.
[511] Glynn and Rogers (n 502) Appendix B- Standard U.K. "All Risks" Policy Form (Business Interruption).
[512] ibid Definitions 1.

5.11. Another distinction between the UK and the US Business Interruption forms is the reliance on a formula for the calculation of the loss to the assured due to or in consequence of the business interruption. The UK form relies on a formula written in the assured's policy which is either on the "Additions Basis"[513] or Difference Basis"[514]. Conversely, the US forms do not include a formula explaining how the gross earning / business income should be calculated.[515] A similar feature of both the U.K. and the US forms is the inclusion of the increased cost of working (ICOW) clause and extra expense clause respectively. Each is created to cover the additional expense reasonably and necessarily incurred to reduce the loss to the business operations caused by or in consequence of the damage to the business premises.[516] In the UK policy, there is an economic limit attached to how much the insurer is willing to pay as 'increased cost of working'.

5.12. The assured may include an additional cost of working (ACOW) clause as an extension to its BI policy, the difference between ICOW and ACOW is that there is no economic limit to the latter. Both the ICOW and the ACOW usually align with the maximum period of indemnity and thus will expire at that agreed date and time. As it relates to the extra expense clause in the US forms, this will come to an end when the repairs or reinstatement of the business have been completed, notwithstanding the continuing losses which the business may still be incurring beyond the completion date. If the assured requires an indemnity beyond the recovery period under the US forms, he will need to purchase an extension through an "extended business income clause" or "an extension of the period of indemnity".[517] Finished Stock is treated differently under each policy.

---

[513] Additions Basis is calculated by adding standing charges to net profit.

[514] The Difference Basis is calculated by subtracting variable costs of production from turnover. This method of calculation provides cover for wages, overheads and net profits. This according to Riley may be the main reason why the Difference Basis of calculation is the preferred method used by BI insurers within the U.K.
Roberts (n 505) para 1.7.

[515]Ibid; Glynn and Rogers (n 502) Appendix C – U.K. Business Interruption ("Difference Basis") Specification "Gross Profit" Wording —Sum Insured Basis and Appendix D the U.K. Business Interruption ("Difference Basis") Specification "Gross Profit" Wording – Declaration Linked Basis are examples of the formula for the calculation of gross profit in the UK BI policy forms.

[516] Neil Greaves and Jo Suppiah, 'Gross Profit – UK vs. Gross Earnings- US' (Marsh Risk Consulting 2013) <https://www.oliverwyman.com/content/dam/marsh/Documents/PDF/UK-en/gross%20profit%20vs%20gross%20earning%2005-2012.pdf >accessed 19 September 2022;
Swiss Re, 'Business Interruption Insurance: every choice has a consequence' (26 June 2018) <https://corporatesolutions.swissre.com/insights/knowledge/business_interruption_insurance_every_choice_has_a_consequence.html> accessed 19 September 2022.

[517] Swiss Re (n 516).

Under the U.K. form, loss to the assured directly or in consequence of loss or damage to the assured's finished stock are covered. Conversely, such losses are excluded in the US forms.[518]

5.13. To make a claim for business interruption, five conditions must be met, each of which will be discussed in alternate order[519]1) BI loss must be caused by an insured peril to property used for the purpose of the business; 2) the material damage proviso must be fulfilled; 3) disruption must be caused by an incident as defined in the policy which causes damage or loss to property; 4) policy must include a material damage clause protecting the insured's property and 5) disruption to the business must have caused damage or loss to the property.[520] First, the BI must be the result of loss, destruction or damage by a peril covered by the insurer in the policy to the property used by the assured as the premises for the purpose of the business. Though generally perceived as correct, this requirement where property damage and business interruption insurance are inextricably linked does not accurately reflect the position as it relates to cyber risk business interruption policies, particularly those which are not a hybrid of property and business interruption. Where the loss, destruction or damage is non-physical, it is unlikely that such will be covered by the insurer of the property used by the assured as the premises for the purpose of the business. In fact, as mentioned throughout this thesis, cyber risks are often excluded from property insurance. So, there will be instances where the interruption to a business is completely non-physical and may for example be caused by DOS attack, yet the protection / indemnity an assured expects from his property insurer will not be met either because there was no evidence of physical damage to the insured property, or the peril was excluded under the property damage policy. Therefore, while there is usually a close link between property and business interruption policies, often demonstrated through the inclusion of a material damage proviso in business interruption policies, these are not present in cyber business interruption policies.

The second condition is that the material damage proviso must be fulfilled. The applicability of a material damage proviso was discussed in *Glengate KG – Properties Ltd v Norwich Union Fire*

[518] Greaves and Suppiah (n 516) 2-3.
[519] With emphasis on conditions 1 and 2, since conditions 3 – 5 are related to conditions 1 and 2 so there would be overlaps if they were discussed in further detail.
[520] Roberts (n 505) para 2.9; Glynn and Rogers (n 502) para 2.3.

Insurance Society Ltd and Others[521] The Claimant, Glengate KG operated business as property owners and developers. Glengate KG purchased the former Bourne & Hollingsworth department store in Oxford Street, London with the intent to develop it to office and retail outlets. Two policies were purchased to insure the building; 1) a material damages policy and 2) a consequential loss policy; the Defendant Norwich Union was the insurer. The Claimant purchased old architect designs for the property which saved them time and money. To prevent delays to work being done, the Plaintiffs created an office space on the property so all the persons working could coordinate and complete the task efficiently. A fire broke out and damaged much of the building and destroyed large numbers of the architects' plan and designs which led to 22 weeks delay. The architects did not have copies of the work in progress and due to an oversight by the architect's brokers, they were uninsured. Glengate KG submitted a claim to the Defendant insurers for their loss. This was rejected by the insurers, who in their arguments referred to memorandum 2 of the material damage policy (below) which included the words *'…the property of the Insured or for which he is (they are) responsible at the site of the aforesaid building(s) and used in connection therewith.'* By this, the insurers contended that the architect's drawings in progress were not property of the assured nor were they responsible for it. Furthermore, Glengate KG could not rely on the material damage proviso since they did not insure the architecture drawings that were in progress as required under the material damage proviso.

5.14. By the consequential loss policy, Norwich Union agreed that if during the currency of the policy:

> any building or other property or any part thereof used by the Insured at the premises described in the Schedule hereto for the purpose of the Business suffers Damage other than by an excluded cause, [it would] pay to the Insured the amount of loss resulting from interruption of or interference with the Business carried on by the Insured at the Premises in consequence of the Damage (such loss being hereinafter termed Consequential Loss) in accordance with the provisions contained in Section 2 of the specification forming part the Schedule …[522]

The consequential loss policy was subject to two (2) provisos. Proviso two (2) read as follows:

[521] [1996] 2 All ER 487.

[522] *Glengate KG* (n 521) 491-492.

> '**In respect of the insurance under Section 2, at the time of the happening of the Damage there shall be in force, under Section 1 or otherwise, an insurance covering the interest of the Insured in the property at the Premises against such Damage and that** (i) payment shall have been made or liability admitted therefor, or (ii) payments would have been made or liability would have been admitted therefor but for the operation of a proviso in such insurance excluding liability for losses below a specified amount.[523]

A typed memoranda was attached to the material damage policy. Memoranda 2 provided:

> The insurance by Item No 2 of this policy extends to include so far as the same are not otherwise insured temporary erections, plant, equipment, tools and materials (including printed books, unused stationery, plans and designs and other contents of temporary offices) **the property of the Insured or for which he is (they are) responsible at the site of the aforesaid building(s) and used in connection therewith.** The liability of the Company under this Memorandum and the policy in respect of any item shall in no case exceed the sum insured by such item.[524]

The issue before the court and of relevance to this discussion was 'whether the drawings were property used by the assured at the premises for the purpose of the business?' As it relates to this first issue, the court rejected the insurers argument and held that the architects' drawings were in fact property used by the assured at the premises for the purposes of the business. Neil LJ reasoning was based on the nature of the plaintiff's business as a property development company that relied on the employment of several independent contractors who designed and constructed the buildings. Neil LJ explained that "the word 'property' and the context in which it was used in the consequential loss policy could not properly be restricted to property owned or in the possession of the assured. The architects' drawings formed an integral part of the assured's business and are accepted as property used by the plaintiff at the premises for the purposes of the business. It would be absurd if in this type of business and the policy written that 'property' would be given any other meaning.[525] As such, the provisions of the consequential loss policy came into effect as the drawings that were damaged were being used by the insured at the premises for the purpose of the business. The reasoning indicates that when deciding whether the property damaged was being used for the purposes of the business, consideration must be given to the nature of the business and the context in which such property is referred in the policy.

[523] *Glengate KG* (n 521) 492 (emphasis added).
[524] ibid 491 (emphasis added).
[525] *Glengate KG* (n 521) 495.

5.15. The second issue that is of relevance to this discussion relates to the material damage proviso 2, the material words of which provides:

> In respect of the insurance under Section 2, at the time of the happening of the Damage there shall be in force, under Section 1 or otherwise, **an insurance covering the interest of the Insured in the property** at the Premises against such Damage…[526]

The issues are: 1) what are the effects of the record drawings not being insured by Glengate KG and 2) whether Glengate KG had an interest in the architects' drawings within the meaning of the proviso?' Rather than relying on the de minimis principle as done by the judge in the lower court, Neil LJ decided that he would accept the alternate arguments of Glengate KG in that on its true construction, the material damage proviso was concerned with the 'property' which caused the consequential loss. It was the destruction of the architects' work in progress which caused the delay. These were the architects' drawings unlike the record drawings which were Glengate KG's. In resolving the second issue, attention must be placed on these words in the material damage proviso, 'interest of the insured in the property' which are to be interpreted only as the assured personally owning the property. Conversely, 'interest' could take on the wider meaning used in insurance[527] and not being limited to property owned by the assured but extends to those which he has a contractual right if the goods were lost or damaged. Based on the foregoing, it was decided that Glengate KG did not need to satisfy the proviso as they had no interest in the architects' drawings that were destroyed in the fire even though it might have a license to use the designs and might eventually acquire the property in the drawings. However, at the time of the fire, the drawings were still the property of the architects, and it was their responsibility to insure them in reference to memorandum 2 of the material damage loss policy. Accordingly, the material damage

---

[526] *ibid*.

[527] *Lucena v Craufurd* (1806) 2 Bos & PNR 269, 302; 127 ER 630. 'A man is interested in a thing to whom advantage may arise or prejudice happen from the circumstances which may attend it; … interest does not necessarily imply a right to the whole, or a part of a thing, nor necessarily and exclusively that which may be the subject of privation, but the having some relation to, or concern in the subject of the insurance, which relation or concern by the happening of the perils insured against may be so affected as to produce a damage, detriment, or prejudice to the person insuring: and where a man is so circumstanced with respect to matters exposed to certain risks or dangers, as to have a moral certainty of advantage or benefit, but for those risks or dangers he may be said to be interested in the safety of the thing. To be interested in the preservation of a thing, is to be so cirumstanced (sic) with respect to it as to have benefit from its existence, prejudice from its destruction...' (Lawrence J).

proviso did not operate as an exclusion to the indemnity to be paid to Glengate KG as the 'architects' drawings were not property in which Glengate had a personal interest and they were under no obligation to insure the architects' drawings themselves'.[528]

5.16. More recently in *The Financial Conduct Authority v Arch Insurance (UK) Ltd (FCA v Arch (UK)*[529], the Supreme Court agreed that a successful claim for business interruption without physical damage is possible based on the context and specific policy wordings. In support of their case that policyholders could recover for business interruption losses resulting from COVID-19 and the public health measures taken by the UK Government, the FCA relied on the interpretation of either the notifiable disease clause[530], hybrid clause[531] or prevention/denial of access clause[532] found within the commercial policies of Defendant insurers. None of the policyholders suffered

[528] *Glengate KG* (n 515) 498 - 499.

[529] *[2021] UKSC 1; [2021] Lloyds Law Rep. IR 63.* A test case (pursuant to the Financial Markets Test Case Scheme) in which FCA initiated proceedings against a group of insurers (Arch Insurance (UK) Ltd, Argenta Syndicate Management Ltd, Royal & Sun Alliance Insurance PLC, MS Amlin Underwriting Ltd, Hiscox Insurance Co Ltd, QBE UK Ltd) in the Commercial court asking the court to make declarations about the meaning and effect of the relevant policy wordings. The case arose from the impact of COVID-19 on the businesses of policyholders, the majority being small and medium sized enterprises. In response to the COVID-19 outbreak and efforts to curtail the risk to the public, the government imposed a series of restrictions which eventually led to many businesses being interrupted or completely closed. As a result of these combined events, the assureds made claims to their insurers for the business interruptions losses they incurred. Thousands of these claims were rejected on the ground that they do not cover pandemic related business interruption. Due to the importance of the issues and the need to urgently settle the matter, the FCA initiated proceedings in the Commercial Court. With the permission of the court, the parties appeal to The Supreme Court.

[530] These clauses generally provide insurance cover for business interruption loss caused by occurrence of a notifiable disease at or within a specified distance of the policyholder's business premises. An example of this is the "Infection Diseases" extension clause found in the business interruption section of the RSA 3 combined commercial policy referred to in the case and which is reproduced here: " We shall indemnify You in respect of interruption or interference with the Business during the Indemnity Period following: a. any i. occurrence of a Notifiable Disease (as defined below) at the Premises or attributable to food or drink supplied from the Premises;… iii. occurrence of a Notifiable Disease within a radius of 25 miles of the Premises…" *FCA v Arch (UK*) (n 529) [4], [48] – [49].

[531] They combine the main elements of disease and prevention of access clauses. An example of this is Hiscox 1- 4 reproduced here: "losses resulting solely and directly from an interruption to your activities caused by your inability to use the insured premises due to restrictions imposed by a public authority during the period of insurance following an occurrence of any human infectious or human contagious disease, an outbreak of which must be notified to the local authority". *FCA v Arch (UK*) (n 529) [4],[96].

[532] The denial of access / prevention of access clauses generally provide cover for business interruption losses resulting from public authority intervention preventing or hindering access to, or use of, the business premises. An example of this is Arch (prevention of access clause) produced here: ""loss … resulting from … Prevention of access to the Premises due to the actions or advice of a government or local authority due to an emergency which is likely to endanger life or property." *FCA v Arch (UK*) (n 529) [4], [96].

any type of physical or tangible loss to property, instead their businesses were interrupted due to COVID-19 and regulatory measures put in place by the government in response to the pandemic. Though the peril in this scenario is not a notifiable disease,[533] the DOS shares similar characteristics, the obvious being its nonphysical nature. The DOS attack which caused the port system to be disabled is comparable to the physical denial of access clause because in both situations the assureds and their customers were prevented from accessing and operating their business. In fact, the emphasis throughout the case was not on the presence or absence of physical damage, rather attention was placed on the meaning of the words used in the relevant policies based on the principles of constructive interpretation and the intention of the parties to the insurance contract.

5.17. On another note, the statement that 'the loss, destruction or damage must be caused by a peril covered by the insurer' does not accurately reflect the causal connection required when seeking to establish that there has been an interruption to the business from a cyber-attack. Some policies are worded so insurers cover only loss, destruction or damage directly caused by a cyber-attack / incident, while for others, insurers are also willing to cover loss, destruction or damage even where it is indirectly caused from, arising from or inconsequence of a cyber-attack /incident. However, Lord Hamblen in *FCA v Arch (UK)*[534] clarified that 'the court does not find it profitable for shades of semantic difference in the interpretation of these phrases; "as a result of", "arising from" and "in consequence of' when either or all are the required causal connection to be established between the occurrence of an insured peril and the interruption of the business before an indemnity will be paid by the insurers. Scrutton J in *Coxe v Employers Liability Assurance Corp Ltd*[535] made the same point when he expressed:

> The words in the condition 'caused by' & 'arising from' do not give rise to any difficulty. They are words which always have been construed as relating to the proximate cause…

5.18. Another requirement is that the property described at 1) must bear the address that has been specified in the policy or its schedule. The policy will cover extensions or new premises and capital

[533] Please see paragraph 5.19. below for an explanation of what constitutes a notifiable disease.
[534] *FCA v Arch (UK*) (n 529) [162].
[535] [1916] 2 KB 629, 634.

equipment only when it has been 'used' by the assured in accordance with the terms of the policy. On the other hand, if there has been loss, destruction or damage to the business of any of the assured's suppliers which have caused or contributed to a reduction in the turnover of the assured business, such loss will only be covered if it is specifically included in the policy under a business contingency clause. This limits the potential liability of the insurer to only damage or destruction to the property agreed between the parties, thereby excluding other properties owned by the assured at other addresses or near the insured property. Many policies mention the term 'Premises' which often refers to the address in the schedule. Merely providing the address in the schedule may lead to uncertainties, resulting in questions such as 'whether the policy was intended to cover an entire site or just the buildings on it, only a floor or the floor and its other common areas or the whole building, a unit, or the whole mall? Does the damage to stock outside the buildings but within the curtilage constitute damage at the premises and how is premises defined for concessions or mini stores within a supermarket or department store?'[536] Answering these types of questions will help to eliminate ambiguities in the interpretation of the insurance contract.

If "premises" or "property" is to be given a wider or more restrictive meaning, this must be specifically stated in the policy, otherwise the parties may disagree over whether the material damage proviso has been satisfied. This requirement remains the same even when the "property" or "premises" is described in a cyber business interruption policy. In fact, the capacity of a cyber-attack to cause damage to a wide area is impetus for the parties to be very precise in what exactly property or premises as used in the policy should mean and include. The *FCA v Arch (UK)*[537] judgment discusses the meaning that should be given to the words, "occurrence…within a 25-mile radius" which is an extension of the property or premises that the policy was intended to cover. The disease clauses, for example RSA 3 "Infectious diseases" extension clause (reproduced below) provides insurance cover for business interruption due to a notifiable disease within a specified

[536] Damian Glynn, Sue Taylor and Steven Nock, *CILA- The Basic Business Interruption Book* (Witherby Publishing 2020) 15-16.

[537] *FCA v Arch (UK*) (n 529) [61]. "No reasonable reader of the policy would the words "any occurrence of a Notifiable Disease within a radius of 25 miles…" to include any occurrence of a Notifiable Disease outside a radius of 25 miles. To seek to interpret the language of the policy as bearing such a meaning is to stand the clause on its head." In other words, it is only an occurrence within the specified area that is an insured peril and not anything that occurs outside that area.

distance. A typical cyber endorsement clause is similar in that like the notifiable disease clause, it is a non-physical cause of business interruption covered through an extension clause attached to a traditional business interruption or commercial policy. The disease clause from RSA 3 will be used as the model clause throughout this discussion. It provides:

> We shall indemnify you in respect of interruption or interference with the Business during the Indemnity Period following … occurrence of a Notifiable Disease within a radius of 25 miles of the Premises...[538]

The issue for the court was to examine what is meant by the words 'following … occurrence of a Notifiable Disease within a radius of 25 miles of the Premises…' and the scope of such provision? In the lower court, RSA insurers proposed that the clause should be interpreted as only covering the business interruption consequences of any case of a notifiable disease that occur within a 25-mile radius of the insured property. Conversely, FCA contended that the clause should cover the business interruption consequences of a notifiable disease wherever they occur provided at least one case of the illness occurs within 25 miles of the insured property. The commercial court accepted the approach taken by FCA and held that 'RSA 3 provides cover for business interruption consequences of a notifiable disease where there has been at least one instance within the specified radius from the time of that occurrence.'[539]

5.19. The correct interpretation is that the clause will 'cover only an occurrence of a notifiable disease within the specified area that is an insured peril and not anything that occurs outside that area'.[540] By arriving at this conclusion, Lord Hamblen rejected the interpretation proposed by FCA and adopted that of the lower Court by clarifying that 'the clause does not mean that there is cover for an occurrence some part of which is within the specified 25 miles.'[541] The term occurrence was construed as 'something that happened at a particular time, at a particular place and in a particular way thus a disease that spread was not something that occurred at a particular time and place in a particular way'.[542] Notifiable disease as defined in the RSA policy does not refer to a disease in

[538] *FCA v Arch (UK*) (n 529) [50] – [41].
[539] *FCA v Arch (UK*) (n 523) [55].
[540] Ibid [65].
[541] Ibid.
[542] *FCA v Arch (UK*) (n 523) [67]-[68].

the general sense. Instead, 'notifiable disease' refers to an 'illness sustained by any person resulting from…' Thus, it is not the outbreak nor the disease itself which is the "notifiable disease", but the illness sustained by any person resulting from that disease".[543] Accordingly, an outbreak of COVID-19 cannot be an occurrence, instead each case of illness sustained by an individual must be treated as a separate occurrence. In plain language, 'the clause only covers cases of illness resulting from COVID-19 that occur within the 25-mile radius specified in the clause.'[544] Lord Hamblen concluded the discussion by stating:

> We conclude that the disease clause in RSA 3 is properly interpreted as providing cover for business interruption caused by any cases of illness resulting from COVID-19 that occur within a radius of 25 miles of the premises from which the business is carried on. The clause does not cover interruption caused by cases of illness resulting from COVID-19 that occur outside that area.[545]

5.20. In the end, it was made unequivocally clear that extending the geographical scope of the cover beyond the area specified in the policy is not acceptable. This would place greater liability on the insurers than was initially agreed when the premium was negotiated resulting in underinsurance and delays in payout. Such a situation was envisaged by Lord Mustill in ***Charter Reinsurance Co Ltd v Fagan*** when he stated:

> There comes a point at which the court should remind itself that the task is to discover what the parties meant from what they said, and that to force upon the words a meaning which they cannot fairly bear is to substitute for the bargain actually made one which the court believes could better have been made. This is an illegitimate role for a court.[546]

Even with a cyber-attack such as the DOS on the port of Liverpool, it is important to carefully analyse the insuring clause and correctly identify the geographic scope of the policy. Will the insurers cover the loss caused to all the businesses at the port or will the port operator be indemnified for specific loss in particular areas of the port? Does the definition include the outbuildings or storage facilities beyond the perimeters of the address provided in the schedule? Such questions are appropriate for those rare occasions when it is established that a cyber-attack has caused damage to a building or tangible property which has led to the interruption of the

[543] ibid [70].
[544] *FCA v Arch (UK)* (n 523) [71].
[545] *FCA v Arch (UK)* (n 523) [74].
[546] [1997] AC 313, 388.

business. The question however changes when like the facts of this scenario, there is no evidence of physical damage, but there exists a denial of access to the port system. How will premises be defined? The points made in relation to the description or definition of premises remains applicable to cyber risk however the triggers may be separately defined in the policy wording.[547] The damage or interruption must still concern the disruption or failure of the assured's or company's IT system or network. Clarifying these points by ensuring the premises is described in detail and accurately means there will be minimal disagreement over whether cover is triggered or not and the extent of coverage available.

5.21. The third condition that must be satisfied to claim for business interruption is that the disruption to the business must be due to an incident as defined in the policy which causes damage or loss to the property. There is no legal or contractual requirement for the property or building to be owned by the assured, it is enough if it is property the assured leases to carry out the specific

[547] Policies vary as to the period when insurers will begin to accept liability for business interruption. Traditional business interruption policies will become operational only when there has been damage or loss to physical property at premises covered by the policy which has caused an interruption to the assured's business resulting in financial loss to the assured. On the other hand, most Cyber risks business interruption policies (CRBI) provide that insurers obligation to indemnify the assured will commence either 'when the computer system first becomes imperiled (sic) or when there is a network failure, interruption or degradation or at the first sign of a data breach.' (Roberts (n 499) para 16.10). The degradation or failure in the network performance being the cause of the loss. Identification of these commencement triggers are not easily ascertained, and the assured could lose significantly before any of these indicators become noticeable. This implies that CRBI will only be triggered when the damage may already be significant and assured may be left without protection for the losses incurred prior to the commencement of the policy. Early detection of the risk is therefore crucial and is in the interest of both the assured and the insurer in reducing liabilities / losses. Equally difficult is understanding when a cyber event has ended, that is when systems have been repaired or restored to pre breach status The ability of hackers to act surreptitiously and for other cyber risks to go undetected for extended periods within a computer system is the result of multiple factors. These include the very advanced and expert techniques being utilised by the hackers who sometimes study company websites and databases for very long to identify their vulnerabilities. Furthermore, some hackers have inside knowledge of the IT operations of their target and on some occasions collaborate with insiders to manipulate the company network. Another reason, detection of a cyber breach may take long is the lack of or minimal training of the assured and his employees to recognise signs of a cyber breach or even vulnerabilities within systems. This is more challenging for SME which may not have dedicated IT personnel to address these issues. Although these issues remain on an assured's list of concerns, it is expected that the detection period will reduce significantly since *IMO Resolution MSC. 428 (98)* makes it mandatory as of January 1, 2021, that each company within the maritime sector appropriately addresses cyber risks in their safety management systems which includes pre breach penetration testing and post breach support.

business stipulated in the policy[548]. Furthermore, property includes tools, equipment and stock that have been affected by the incident. Fourthly, the policy must have a material damage clause protecting the assured's property against loss, destruction, or damage. The insurer must accept that there is material damage to the assured interest.[549] Fifthly, the disruption to the business must have caused damage or loss to the property. In relation to the DOS attack on the port of Liverpool, what exactly will qualify as damage or loss? Usually, "Damage" with a capital 'D' is defined in traditional policies and includes direct physical loss, accidental or non-accidental destruction or damage to property insured.[550] In other instances damage without a capital D is given a wider meaning to include non-physical damage or loss to property for example loss or damage due to a denial of access to the property. Ultimately, the definition or interpretation of 'damage or loss' will depend on the exact words of the policy.

II. Insurance implications of the cyber-attack on the ports of Liverpool

5.22. There are varying losses arising from this scenario and the extensive list include business interruption, contingent business interruption, cargo losses, regulatory breaches and defence cost, reputational risk, data and possibly software losses. The focus of the discussion will be on business interruption and reputational risk as the other losses have been covered in previous scenarios. Particular attention will be placed on the standard U.K Business Interruption policy forms and the traditional marine insurance policies to determine how they will respond to the losses highlighted in the scenario. Finally, there will be an evaluation of some of the cyber insurance policies available in the market and how well they would respond to the risks and liabilities arising directly and indirectly from the cyber-attack on the Ports of Liverpool.

[548] *Mark Rowlands v Berni Inn* [1986] Q.B. 211 confirmed that a tenant does have an insurable interest in the property he leases. There is still uncertainty as to whether the tenant would need to take out his own material damage cover or if the presence of this proviso under the landlord policy is sufficient to protect the tenant's business interruption risks. Compare Roberts (n 505) para 2.11 and *Glengate-KG Properties v Norwich Union Fire Insurance Society Ltd* [1996] 2 All E.R. 487 where it was concluded that the proviso could only be concerned in that which the insured had personal property interest and which it could reasonably be expected to insure.

[549] Roberts (505) [2.9].

[550] CILA & Insurance Institute of London (n 501).

A. Standard U.K "All Risks Policy Form (Business Interruption)

Standard U.K. "All Risks" Policy Form (Business Interruption)

> The Insurer agrees (subject to the terms, definitions, exclusions and conditions of this policy) that if after payment of the first premium **any building or other property used by the Insured at the Premises for the purpose of the Business be accidentally lost destroyed or damaged during the period of insurance** (or any subsequent period for which the Insurer accepts a renewal premium) and in consequence the business carried on by the Insured at the Premises be interrupted or interfere with then the Insurer will pay to the Insured in respect of each item in the Schedule the amount of loss resulting from such interruption or interference provided that…[551]

a. Damage to building or other property: Are Data, Software and Cargo losses covered?

5.23. The Standard U.K "All Risks Policy Form (Business Interruption) includes conditions that must be satisfied to trigger the operation of the policy and before the insurer accepts any liability under the policy. The first requirement is that there must be damage or loss to the building or other property used by the insured at the premises for the purpose of the business. The facts in this scenario did not include / make reference to damage to building or any other premises used for business so any submission in relation to damage or loss to a building can be easily discarded. However, the reference to 'building or other property' may create some difficulty in interpretation for both the assured and the insurer. Will 'other property' include the damaged data or software that has been lost due to the DOS attack at the port of Liverpool?[552] If the specific word 'building' is to govern the meaning of 'other property', it suggests that the existence of a physical state or characteristics similar to a building is essential to the definition and acceptance of what insurers would classify as 'property'. Therefore, since data and software do not occupy a physical state or share the characteristics of a building, it is improbable that 'data and software' will be covered in this clause. If the emphasis is shifted from the presence of the word 'building' and focus is placed on 'other property', it is arguable that damage to software which is stored on some physical device for example a USB could equate to damage to property, sufficient to qualify under the material damage proviso in traditional business interruption policies.

[551] Glynn and Rogers (n 502) Appendix B- Standard U.K. "All Risks" Policy Form (Business Interruption).
[552] See discussion on this issue at paragraph 2.55. -2.56.

5.24. Furthermore, the building or other property must be 'accidentally lost destroyed or damaged during the period of the insurance'. The key word here is 'accidentally' which was not defined in the policy but by its natural meaning indicates a lack of intention or something done inadvertently or by chance. There are two potential arguments; the insurers may develop their defence by arguing that the ports of Liverpool were the targets of the DOS attack thus it was not an accident as required under the policy. A DOS by its nature is directed at an identified victim, in this case the port network. Alternatively, the insurers may reason that a breach of a computer network being operated on an outdated system is foreseeable thus it is mute to argue that the DOS and consequent BI was an unexpected accident. From the assured's perspective (port operators, ship owners and cargo owners) the DOS attack on the ports of Liverpool is a 'fortuitous happening'[553] and thus should be treated as an accident. Mustill LJ in *De Souza v Home and Overseas Insurance Co Ltd* explained that '[T]he word "accident" involves the idea of something fortuitous and unexpected, as opposed to something proceeding from natural causes'.[554] The assureds may also rely on the fact that the DOS attack affected not only the ports of Liverpool but all users of the outdated Windows 2000, to support their point that the DOS was an accident and not a targeted attack. Besides, the DOS was not an incident that the port operators expected otherwise they would have taken the precautionary measures to prevent and mitigate the impact on the port, its customers and supply chain. Moreover, it did not occur from natural causes or from foreseeable consequences thereof.

Rather than trying to dissect the meaning of these terms and debating whether 'software' or 'data' qualifies as 'other property', parametric insurance for cyber business interruption will help to resolve these issues since there is no need to prove damage to or loss of property.[555] The effect of parametric insurance is that instead of operating on an indemnity basis, the insurer will automatically pay if the critical IT services of the assured have been disrupted or the agreed policy

[553] *TKC London Ltd v Allianz Insurance Plc* [2020] EWHC 2710 (Comm); [2020] Lloyd's Rep. IR 631 [51].

[554] [1995] LRLR 453, 458.

[555] Swiss Re Corporate Solutions, 'Innovating\ Together Innovative Risk Solutions' (nd) 24 <https://corporatesolutions.swissre.com/dam/jcr:34fb5129-15c8-4265-80fd-a27f739fb8f0/innovating-together-examples-innovative-risk-solutions.pdf> accessed 25 September 2022.

triggers activated.[556] It is important to identify what is agreed to be critical IT service between the parties and the shipping industry generally but these could include the cloud, client and cargo databases and electronic payment systems. Critical IT services of the ports of Liverpool will certainty include its port management and computer system network which control, monitors and facilitate all operations around the port and communication among stakeholders including those along the supply chain.

5.25. Containers packed with various types of cargo were stolen following the denial-of-service attack at the Ports of Liverpool. The DOS attack which exposed the vulnerability of the port's computer network was the most efficient or proximate cause of the cargo theft, hence property loss in the context of the form. Even though the cargo loss or damaged during the attack is property based on the conventional meaning of the term, it may not qualify under the Standard U.K All Risks Business Interruption form since the cargo was not being used by the assured at the premises for the purpose of the business. As discussed above[557] the phrase 'use for the purpose of the business' will depend on the nature of the business. Among the services provided by port operators is the transit and temporary storage of cargo in warehouses or other storage facilities located at the property. Even if it is to be accepted that such services qualify as 'use for the purpose of the business', it is debatable whether cargo being stored at or transiting the port equates to 'use…' by the insured? Certainly, the answer will depend on the definition given to 'insured / assured'. Insured / Assured is not defined in the form but if it includes cargo owners, this will need to be expressly provided. However, such clarification would not alter the outcome since the interruption to the operations at the Ports of Liverpool was not in consequence of the lost cargo. Reference to the phrase 'and in consequence the business carried on by the Insured at the Premises be interrupted or interfered with…' as provided in the introductory paragraph of the Standard U.K "All Risks

[556] Lloyds, 'Lloyd's launches "first-of-its-kind" business interruption insurance policy' (30 September 2020) <https://www.lloyds.com/about-lloyds/media-centre/press-releases/lloyds-launches-first-of-its-kind-business-interruption-insurance-policy> accessed 25 September 2022. This type of insurance is geared towards small and medium sized businesses and designed to reduce the time and expense of the claims process. It is not to replace traditional policies but to complement them by filling gaps in coverage.
Swiss Re Corporate Solutions, '10 myths about parametric insurance' (15 July 2022) <https://corporatesolutions.swissre.com/insights/knowledge/10_myths_about_parametric_insurance.html> accessed 25 September 2022.

[557] See paragraphs 5.23 – 5.24.

Policy Form (Business Interruption) (cited above) requires that the lost, destruction or damage to any building or other property used by the assured for the purposes of the business is the proximate cause of the business interruption. By applying the principles to the facts, the interruption of the businesses at the port must be in consequence of the loss of the cargo. In other words, the lost cargo must be the cause of the business interruption at the Ports of Liverpool. However, the facts do not support that conclusion because the loss of the cargo (other property) was not the cause of the interruption or interference rather, the cargo was lost as a consequence of the DOS to the ports' computer network. The same point was made by Richard Salter QC in ***TKC London Ltd v Allianz Plc***[558] where he held that:

> The Business Interruption Section of the Policy responds to "Business Interruption by any Event". The word "by" in that phrase connotes causation, and the definition of Business Interruption itself requires the interruption or interference to be "in consequence of an event to property used by the Insured at the Premises", a phrase which (as Mr Kealey QC submitted) commonly denotes proximate causation.
> …The deterioration of TKC's stock during the period of closure did not cause TKC's business to be interrupted or interfered with, because (as is common ground) it occurred at a point at which that business was already closed a s a result of the Coronavirus Regulations. It was a consequence of the interruption or interference, not its cause.

Based on the foregoing, The assured port authority cannot depend on their business interruption policy to satisfy any claim against them by carriers and cargo owners for the damage or loss of cargo that was being stored or transiting through the port at the time of the attack.

5.26. Port operators have an obligation to provide a safe berth / port. Though this is unrelated to the business interruption claim, it is foreseeable that carriers may argue that the port breached their contractual obligation to do so. The recurring cybersecurity breaches at the Ports of Liverpool support the point that the port is unsafe. Moreover, the recurring breaches are cogent evidence to support the inference that the port operators have not taken the necessary measures to protect the port against cyber-attacks, thus the port may be rendered unsafe.[559] An unsafe port was defined by Sellers LJ in *The Eastern City*:

---

[558] *[2020] EWHC 2710 (Comm); [2020] Lloyd's Rep.* IR 631 [110] – [111].
[559] *Ocean Victory [2017] UKSC 35; [2017] 1 Lloyd's Rep* 521.

> A port will not be safe unless, in the relevant period of time, the particular ship can reach it, use it and return from it without, in the absence of some abnormal occurrence, being exposed to danger which cannot be avoided by good navigation and seamanship ...[560]

The relevant question at this stage is whether a vessel can reach the ports, use it and return from it without being exposed to danger and whether the cyber-attacks, taking place within 2 months of each other, should be considered as an 'abnormal occurrence' to negate the position that the ports of Liverpool were unsafe. Both terms "occurrence" and "abnormal" maintain their ordinary meanings. An occurrence 'is an event that happened on a particular time, at a particular place in a particular way'.[561] Abnormal is something out of the ordinary and unexpected.[562] Considering that this was not the first cybersecurity breach within two months, it cannot be said to be an abnormal occurrence especially if appropriate security measures in accordance with the IMO guidelines on maritime cyber risk management[563], ISPS Code[564], NIS Regulations[565] and guidelines from the

---

[560] *Leeds Shipping Company Ltd v Societe Francaise Bunge (The Eastern City) [*1958] 2 Lloyd's Rep 127, 131(CA).

[561] *FCA v Arch (UK*) (n 519) [67].

[562] *Ocean Victory* (n 559) [16].

[563] IMO, 'Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.1)' (14 June 2021) <https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf> accessed 25 September 2022. The includes both guidelines and recommendations on cyber risks management to protect shipping from current and emerging cyber threats and vulnerabilities relating to digitization, integration and automation of processes and systems in shipping as outlined in paragraph 1.2

[564] The International Ship and Port Facility Security (ISPS) Code. The ISPS was first implemented in the UK through EU regulation on enhancing ship and port facility security (725/2004) which has been amended by The Ship and Port security (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019 No. 0308). The text of ISPS Code can be found in Chapter XI-2 of the Convention for the Safety of Life at Sea (SOLAS) 1974 as amended in January 2020. The main objective of the ISPS Code is to establish an international framework involving key stakeholders in the marine sector namely contracting Governments, government agencies, shipping and port industries to detect and assess security threats against port and shipping facility and to take preventative actions against such threats. The preamble of the ISPS Code explains that provisions shall only apply to ship/port interface and not wider issues regarding the security of port area. The provisions will also not extend to the actual response to attacks or to any clear-up activities after an attack. The ISPS Code focuses on the physical security of ports and vessels, however the language employed in some of the provisions (port facility assessments should take account of changing threats and ship and port facility assessments and identification of vulnerabilities should address and consider radio and telecommunication systems, including computer systems and network) denote that the Code is also applicable, even to a limited extent to cybersecurity threats. For a comprehensive discussion on the extent to which the ISPS Code and other international regulations will apply to cyber risks and the recommended actions to strengthen cyber resilience at ports and port facilities, see
The World Bank, 2020. "Accelerating Digitization: Critical Actions to Strengthen the Resilience of the Maritime Supply Chain." World Bank, Washington, DC. License: Creative Commons Attribution CC BY 3.0 IGO
< World-Bank-IAPH-joint-paper-accelerating-digitalization.pdf (sustainableworldports.org)>
accessed 25 September 2022.

[565] The UK Network and Information Systems Regulations came into force on 10th May 2018 to improve security in the network and information systems necessary for the delivery of digital and essential services. It was the domestic implementation of The Network and Information Systems Directive created by the European Parliament in July 2016 and implemented in August 2016 with the objective to improve the security of network and information systems across the EU.

Code of practice on security in ports[566] were not effectively implemented to prevent or minimize the risks of another cyber security breach.

b. Possible exclusions under the Standard U.K "All Risks Policy Form (Business Interruption)

5.27. Satisfying all the conditions mentioned in the introductory paragraph (cited above) of the Standard U.K "All Risks Policy Form" (Business Interruption) does not mean that the assureds' claim will be successful as the policy is subject to the expressed terms, definitions, and exclusions. Even though 'malicious persons' is included in the description of 'defined perils', this does little to advance the claim of the assured in seeking to rely on the fact the persons or entity responsible for the DOS are malicious and accordingly the loss arising directly or indirectly from their actions is a peril covered by the policy. The futility of this argument is based on the exclusion in clauses 5.3 and 10.3 which exempts the insurer from liability due to CONSEQUENTIAL LOSS[567] arising directly or indirectly from

> **5.3 disappearance, unexplained or inventory shortage**, misfiling or misplacing of information
>
> **(a)**erasure loss distortion or corruption of information on computer systems or other records programs or software caused deliberately by rioters strikers locked-out workers persons taking part in labour disturbances or civil commotions or malicious persons
>
> **(b)**other erasure loss distortion or corruption of information on computer systems or other records programs or software unless resulting from a Defined Peril in so far as it is not otherwise excluded
>
> **10. CONSEQUENTIAL LOSS in respect of**

[566] ILO and IMO, 'Code of practice on security in ports' (MESSHP/2003/14, Geneva 2003) <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ILOIMOCodeOfPracticeEnglish.pdf> accessed 25 September 2022. This is a joint publication by the ILO / IMO Working Group on Port Security. It complements the ISPS Code as it provisions extend beyond security of port facilities to the whole port.

[567] The words "CONSEQUENTIAL LOSS", in capital letters, shall mean loss resulting from interruption of or interference with the Business carried on by the Insured at the Premises in consequence of loss or destruction of or damage to property used by the Insured at the Premises for the purpose of the Business. The words "Defined Peril" shall mean fire, lightning, explosion, aircraft or other aerial devices or articles dropped therefrom, riot, civil commotion, strikers, locked-out workers, persons taking part in labour disturbances, malicious persons, earthquake, storm, flood, escape of water from any tank apparatus or pipe or impact by any road vehicle or animal.

10.3 Computers or data processing equipment[568]

Clauses 5.3(a) and (b) and 10.3 operate as cyber exclusion clauses. The 'malicious persons' would be the hackers who deliberately targeted the computer systems of Liverpool Ports. There must be ill will or spite directed specifically at their computer systems[569]; an undirected accidental or coincidental interference with the systems would not be included in the clause.[570] The DOS attack targeted and was spitefully directed at the computer systems of Liverpool Ports to cause harm or disruption, so the hackers are 'malicious persons' as used in clause 5.3(a).[571] When applied to the facts in this scenario, the result is that the delays and interruption to the port operations and all other consequential losses arising directly or indirectly from the erasure loss, distortion, corruption of information on the port computer systems, records program or software that is caused deliberately by malicious persons will not be covered by the insurer. The meaning of 'loss' as used in the phrase 'other erasure loss distortion or corruption…' relates only to loss through electronic interference, therefore the exclusion would not extend to the physical theft of cargo at the port during the period of interruption.[572] Nevertheless, because theft is not listed among the 'Defined perils', the 'loss' of containers or cargo by such means would not be an exception to the exclusion in clause 5.3(b). Even if the exclusions in clause 5.3(a) and (b) are not applicable, clause 10.3 excludes consequential loss arising directly or indirectly from 'computers or data processing equipment', an exclusion wide enough to include the DOS attack on the ports of Liverpool, so that

[568] Glynn and Rogers (n 496) Appendix B- Standard U.K. "All Risks" Policy Form (Business Interruption).

[569] *Atlasnavios-Navegação Ida v Navigators Insurance Co Ltd and Others (The "B Atlantic")* [2018] UKSC 26; [2018] 2 Lloyd's Report 1, para 22.

[570] *Tektrol Ltd v International Insurance Co of Hanover Ltd* [2005] EWCA Civ 845, paras 12, 21, 26.

[571] Ibid, paras 11-12. Generally, hackers are malicious persons but in clause 5.3(a), 'malicious persons' adopts its meaning from the preceding category of persons 'rioters strikers locked-out workers person taking part in labour disturbances or civil commotions'. The judges agreed that based on this list, the draftsmen intended for the interferences to be specifically directed at the assured's computers and committed near or on his premises. If the insurers intended to exclude all damage, however caused by hackers, they needed to place 'malicious persons' in a separate clause and not in the same terms as the other categories of people named. This aspect of the facts distinguishes the scenario from the *Tektrol Ltd v International Insurance Co of Hanover Ltd* where the same clause was included in the policy of Tektrol Ltd. In Tektrol, the source code was lost due to the introduction of a virus on their computer systems after the Managing Director opened an infected email received from a firm of solicitors. The authors of the virus had no knowledge of or connection to Tektrol, therefore Tektrol was not a direct target, and the authors of the virus were not 'malicious persons' within the context of the exclusion relied on by the Insurers. The insurers could not rely on that exclusion to relieve them of liability to Tektrol for the virus damage.

[572] *Tektrol Ltd (*n 570) [27]-[29].

the BI insurer would not be liable to indemnify the Liverpool ports authority for their loss or damage from the interruption.

5.28. Liverpool port authority will need to find an alternative cover and if they had no other insurance at the time of the incident that will accept liability for such losses, they will be expected to cover the costs and expenses without the assistance of an insurer or reinsurance company. This situation puts the port authority in a difficult financial position as they will now be required to allocate monies to replace or restore data including the ship and cargo manifest which have been lost or corrupted on the port computer system and the consequential losses will not be covered by the insurer. This brief analysis demonstrates the inadequacy of standard UK business interruption policies to cover cyber related risks and losses thus an assured will be exposed to liabilities which without a cyber policy or extension he would be expected to pay directly from the business revenue even though the business or in this case the port was not in operation for over 15 days.

B. Cyber Insurance and Business Interruption

a. The nature of cyber business interruption

5.29. As the demand increases for smart and digitalized ports so does the risks of a cyber-attack and the need for cyber business interruption insurance. The interruption of the operations at the ports of Liverpool was caused by a cyber-attack on the port system which was successful primarily because of the vulnerabilities embedded in operating on an outdated Windows system. Traditional business interruption policies do not provide any form of protection or indemnity to the assured for non-physical risk that caused an interruption to their business. This lacuna has been to a great extent addressed by cyber insurance providers. Most cyber insurance policies include a business interruption or network interruption clause intended to protect the assured against direct and consequential losses from interruption to the business arising from a cyber breach.

5.30. The definition given to business interruption varies across policy providers but usually includes loss of income and increased costs of working resulting solely and directly from a partial or total interruption to the assured's business. The calculation of loss of profit in cyber business interruption policies are usually based on either i) a loss of gross profit or ii) a Net Profit or Net

Income plus continuing fixed costs approach.[573] Currently most cyber business interruption policies are written on the Net Profit / Net Income approach but there is an increasing shifts towards the loss of gross profit approach which is widely used in UK property policies.[574] The interruption to the business must have commenced during the period of the insurance and last longer than the time excess. Time excess refers to the hours immediately following for example, the DOS attack during which there will be no insurance cover for any loss the assured experiences because of the attack. In some policies, the time excess does not apply generally, instead the policy will specifically identify the clauses to which the time excess is applicable. It is described either within the business interruption clause itself or in a schedule to the policy and normally lasts between '6 to 72 hours after the start of the incident or less often up to 5 or 7 days'.[575] An example of a time excess clause found in a cyber insurance policy is provided below:

Excess	You must: 1. pay the relevant **excess** shown in the schedule; and 2. bear any loss or expense suffered during the **time excess** in respect of each covered: a. partial or total interruption to **your business**; b. loss under **What is covered**, **A. Your own losses**, Operational error, Dependent business interruption or Reputation protection[576]

If the facts were different and the port network was repaired before the excess period expires, the port operators would not be indemnified for the subsequent business interruption loss. This is based on general insurance practice and sometimes expressed in the policy for example RSA Business Interruption clause reproduced below:

Cyber Risk Insuring Clauses

[573] Ben Hobby, 'Cyber Insurance and Business Interruption' (IUA and RGL Forensics 2018) 6 <https://www.iua.co.uk/IUA_Member/Document_Library/Circulars_2018/IUA_publishes_cyber_insurance_and_business_interruption_report.aspx > accessed 25 September 2022. See discussion below on the features of Net Profit / Net income and Gross Profit approaches to calculating business interruption in cyber policies.

[574] ibid.

[575] Celso de Azevedo, '*Cyber Risks Insurance Law and Practice*' (1st edn, Sweet & Maxwell 2019) para 6-004.

[576] Hiscox Cyber Clear Policy, 'WD-PIP-UK-CCLEAR (1) 19029 12/18' (2018) <https://www.hiscox.co.uk/sites/uk/files/documents/2019-03/19029-CyberClear-policy-wording.pdf > accessed 25 September 2022.

> Subject to payment of all applicable insurance premiums, the Company shall indemnify the Insured up to the Cyber Risk Limit of Indemnity against:
>
> **Cyber Business Interruption**
> Any Business Interruption Loss incurred by the Insured, after the Waiting Period, resulting from a Cyber Business Interruption Event commencing during the Period of Insurance and reported to the Incident Manager in accordance with this Policy.[577]

5.31. Equally important is the indemnity period stipulated as this is a vital factor in determining how much and for how long the insurer will indemnify the assured for his loss. Hiscox CyberClear insurance policy wording defines the indemnity period as 'the period in months, beginning at the date the interruption to your business commences and lasting for the period during which your income is affected as a result of the interruption but for no longer than the number of months shown in the policy.'[578] Another policy describes the indemnity period as "beginning at the end of the Waiting Period, ending when the Business is restored to the same or equivalent condition, functionality and service that existed prior to the Cyber Business Interruption Event, but not exceeding a maximum period of 90 calendar days".[579] Typically, the indemnity period will carry on for the number of hours or days stated in the policy or its schedule. Having explained the key terms, the business interruption at the port of Liverpool will be discussed in relation to the coverage offered under various cyber insurance policies that have emerged in the market. Following this discussion, an assessment will be made as to the adequacy of cyber business interruption insurance for the assured and other stakeholders who have been affected by the DOS at the ports.

b. Cyber Business Interruption – What is covered?

5.32. Port operations have been interrupted for fifteen (15) days, substantially removing the port's source of income. In addition to the direct loss of income by the port operator, there will be similar losses to dependent businesses such as shipowners, cargo owners and other employees

[577] RSA Insurance plc, 'Cyber Risk Insurance Policy Wording: Cyber Business Interruption' (UKC05268A September 2018)<https://www.rsainsurance.co.uk/media/ruhfu0rp/cyber-risk-insurance-policy-wording-ukc05268a.pdf> accessed 25 September 2022.
[578] Hiscox (n 576).
[579] RSA (n 577) General Definitions – Indemnity Period.

working at the ports. Therefore, the loss of income is a major concern and will be an ongoing issue for months possibly years considering there will be reputational damage which will require increased marketing to regain the trust of customers and the various stakeholders along the supply chain. While the port operators and other business dependents may still be losing income in as a result of the cyber-attacks, insurers are not prepared to pay out the exorbitant amounts over an extended period. This is the reason many policies have relatively short indemnity periods when realistically the financial impact may continue well beyond the indemnity period agreed between the insurer and assured.

i. Business interruption losses and loss of income

In this section, I will briefly discuss what constitutes business interruption losses and loss of income as provided in cyber insurance policies. The clause below is an example of a business interruption losses clause, the terms of which will guide the discussion and analysis that follows.

Business interruption losses

A. If during the period of insurance, and in the course of your business or advertising, you discover or reasonably suspect any:

1. breach;
2. security failure
3. illegal threat; or
4. cyber attack against you;

we will pay:

Business interruption losses

e. Your:
   i. loss of income
   ii. increased costs of working; and
   iii. additional increased costs of working, where shown on the schedule;

resulting solely and directly from a partial or total interruption to your business commencing during the period of insurance and lasting longer than the time excess.[580]

[580] Hiscox (n 576).

5.33. As gleaned from the Hiscox CyberClear business interruption clause above, the costs paid for business interruption will include a calculation of the loss of income[581], the increased and the additional increased costs of working[582] where the latter is shown in the schedule. Once a claim has been made for a covered loss such as the disruption to the port operation as a result of the cyber-attack and, provided there are no applicable exclusions[583] or breaches by the port authority that would absolve the insurers of their liability, the insurers agree to pay the difference between the port's actual income during the indemnity period and the income it is estimated the port would have earned (pre-incident) during the same period. From this difference, subtract any savings resulting from the reduced costs and expenses the port would pay out of their income during the indemnity period. The insurers will pay for the increased costs of working.

5.34. Another important observation about the loss of income calculation is the requirement that when applied to the facts of the scenario, the insurers will only pay for loss that is the sole and direct result of the interruption at the port from the DOS attack. In effect, consequential and indirect losses for example losses to dependent businesses or other customers will not be covered by the insurers. The requirement for the loss to be a sole and direct consequence of the breach is a general attribute of business interruption policies written on a loss of income / net profit basis. It is criticized for 'its restrictive benefits to assureds and lack of clarity in calculation of business interruption losses, particularly where net profit / loss of income is not defined in the policies and parties automatically assume, that the terms take the meanings applied in accounts which is not necessary the position in insurance.'[584] One problem is that if the accounting definition of net income / net profit is to be accepted, which generally is 'sales or income minus costs, expenses and taxes of the business', there is no mention of fixed costs such as payroll or other ongoing costs of the business.[585] The non-inclusion of these fixed costs especially when the interruption to the

[581] Ibid. Income is defined as the 'total income of the business, less any savings resulting from the reduced costs and expenses.'

[582] The policy defines Increased costs of working as 'the reasonable and necessary costs and expenses incurred by you (assured) for the sole purpose of minimizing the reduction in income during the indemnity period, but not exceeding the reduction in income saved.'

[583] See discussion on outdated systems exclusion clauses.

[584] de Azevedo (n 575) para 6-007- 6-008. See discussion on the features of Net Profit / Net income and Gross Profit approaches to calculating business interruption in cyber policies.

[585] Ibid.

business is for an extended period of fifteen (15) days means that the scope and adequacy of the insurance coverage is reduced significantly as is the situation at the ports of Liverpool. The lack of clarity in defining these terms and the ambiguity in interpretation increases the risk of underinsurance, thus the premium paid may be inadequate to cover the extent of loss or the claim is reduced if the policy includes an 'average or underinsurance clause'.[586] This reduced scope of coverage is embodied in the overheads and business expenses clause, discussed below. Some policies may not include a similar clause and remain silent on the issue however to guarantee adequate coverage to the business, it is important that fixed costs and other ongoing expenses are included in the calculation of the business interruption losses.

5.35. Interestingly and what will certainly be a concern for the assured is the clause on overheads and business expenses which provides that any amount to be paid by the insurers shall not include or be calculated based on overhead expenses. These types of clauses are typical with the Net Income or Net Profit approach to calculating business interruption and it is for this reason that the clause is found under the Hiscox Cyberclear, 'How much we will pay' heading and reads:

> **Overheads and business expenses**
>
> Any amounts to be paid by **us** shall not include or be calculated based on any of **your** overhead expenses, **your** liability for debt, taxes, lost costs or profits, salaries or wages ordinarily incurred in the performance of **your business**, or any future cost of doing business, including but not limited to the cost of any future licence or royalty, or costs of improving **your** security or performing audits. However, this does not apply to any costs or expenses covered under **What is covered**, **E. Additional covers**, Repeat event mitigation or **What is covered**, **A. Your own losses**, c. Cyber attack losses.[587]

The assured port operators ought not to be alarmed, as there is an inherent limitation to the clause since it does not apply to any costs or expenses under What is covered A. (c) and E, cyber-attack losses or repeat event mitigation respectively (see last line of clause above). The cyber-attack losses sub-clause What is covered A. (c) provides that the insurer will cover:

> additional business expenses, including but not limited to i. the increased cost of power, ii. the increased costs of internet usage; iii. the reasonable and necessary costs to restore your search engine rating and iv. the costs of any malicious pay-per- clicks which (i – iv) are suffered or incurred by the assured as a direct result of a cyber-attack.[588]

[586] de Azevedo (n 575) para 6-009.
[587] Hiscox (n 576).
[588] Ibid (my emphasis added).

The same policy in the Special definitions section defines additional business expenses as 'the reasonable and necessary additional costs incurred as a direct result of a cyber-attack, but not including any normal overhead costs, general business expenses, salaries or wages incurred by you or any other person or entity.'[589] When the overheads and business expenses clause is read in conjunction with the cyber-attack losses clause, the most plausible interpretation is that the insurer will only be liable for the overheads and expenses under two (2) circumstances; 1) where the losses are the direct result of a cyber-attack and 2) for additional covers particularly repeat event mitigation. Even so, there are very specific items listed under the cyber-attack losses, each being a type of utility or service costs which gives the impression that only expenses of this nature, and which are incurred by the assured as a direct result of a cyber-attack will be included by the insurer when the amount to be paid to the assured is being calculated. This interpretation remains the same notwithstanding the use of the phrase 'including but not limited to:' in the opening line preceding the covered expenses listed as i – iv (referred to above).

5.36. The phrase 'including but not limited to' was briefly discussed in ***Markerstudy Insurance Co Ltd v Endsleigh Insurance Services Ltd***[590]. The issue of relevance concerns art 13.1 of the 5th agreement between the parties which excluded liability for 'indirect or consequential loss (including but not limited to loss of goodwill, loss of business, loss of anticipated profits or savings and all other pure economic loss)' arising out of or in connection with the agreement. Markerstudy submitted that art 13.1 only exempted Endsleigh from liability for indirect or consequential loss. Endsleigh disagreed submitting instead that they were exempted not only for indirect and consequential loss but also for direct loss in the categories of loss mentioned in the parentheses. Steel J accepted the submission of Markerstudy on this issue. He held that the specific categories of loss such as loss of goodwill were not freestanding, in the sense that they encompassed all losses within that category whether direct or indirect but were examples of the type of losses making up indirect loss. The point was also made that the use of the phrase "including but not limited to" was a strong pointer that the specified heads of loss were only examples of the excluded indirect loss.

[589] Ibid.
[590] [2010] EWHC 281 (Comm).

Similarly, the specified heads of loss are only examples of the class of business expenses that the insurer will cover in the event of a direct cyber-attack. In any event only the expenses listed i – iv and those related to it will include or be calculated based on 'any of your overhead expenses, your liability for debt, taxes, lost costs or profits, salaries or wages ordinarily incurred in the performance of your business, or any future cost of doing business, including but not limited to the cost of any future licence or royalty, or costs of improving your security or performing audits'. Furthermore, the additional expenses referred to in the policy means 'the reasonable and necessary additional costs incurred as a direct result of a cyber-attack, but not including any normal overhead costs, general business expenses, salaries or wages incurred by you (the assured) or any other person or entity'. So, by the definition of 'additional business expenses' it is evident that the insurer will not include or calculate normal overheads costs, general business expenses salaries or wages when indemnifying the assured for loss of income relating to the interruption to the operations at the port as a direct result of the cyber-attack.

5.37. Another example of a business interruption clause is that found in Beazley Breach Response policy:

> Business interruption loss means:
>
> 1. **income loss**;
> 2. **forensic expenses**; and
> 3. **extra expense**;
>
> Actually sustained during the **period of restoration** as a result of the actual interruption of the **insured organization**'s business operations caused by a **security breach** or **system failure**. Coverage for **business interruption loss** will apply only after the **waiting period** has elapsed.
>
> Business interruption loss will not include (i) loss arising out of any liability to any third party; (ii) legal costs or legal expenses; (iii) loss incurred as a result of unfavorable business conditions; (iv) loss of market or any other consequential loss; (v) **dependent business loss**; or (vi) **data recovery costs**.
>
> Income loss means an amount equal to:
>
> 1. net profit or loss before interest and tax that the insured organization would have earned or incurred; and

2. continuing normal operating expenses incurred by the insured organization (including payroll), but only to the extent that such operating expenses must necessarily continue during the period of restoration.[591]

A noticeable difference between the Hiscox clause on overhead expenses and Beazley's definition of income loss is the treatment of continuing expenses. Under the Beazley Breach Response policy, the assured is in a more favourable position as income loss includes the calculation of normal operating expenses incurred by the assured including payroll, provided that such expenses must necessarily continue during the period of restoration. Overhead expenses, wages and salaries and debts are some of the main expenses that an assured is likely to struggle to pay during a business interruption as the flow of income that would service or supply the financial resources for these expenses have been interrupted. On that basis, it is of little benefit to an assured to agree to a policy with the Hiscox wording on overhead expenses.

To avoid uncertainties and the financial strain on the business, the preferred wording for an assured would be that or similar wording to Beazley income loss definition. In terms of the latter wording, the assured would still be required to understand what exactly is meant by 'such expenses must necessarily continue during the period of restoration'? The period of restoration may vary depending on the insurance provider. However, Beazley policy declares this to be the 180-day period that begins upon the actual and necessary interruption of the business operation. During this period, the assured and insurer combine their efforts to restore business operations to normalcy. The question for the assured to consider is what happens and who will bear the cost at the end of the restoration period? The point has already been made in previous chapters that the impact from a cyber-attack and more specifically a business interruption will not be immediately ascertained. Even though 180 days appears lengthy, it could take investigators longer to identify the source of the attacks not to mention the lingering financial impact beyond this period as it may be impossible to arrive at a definitive figure in such a short time span.

[591] Beazley, 'Beazley Breach Response policy: Insuring Agreement Breach Response' (nd) <https://policies.dppl.com/policy.php?policy_number=BBR-5A8ED7A3-8OEF > accessed 25 September 2022.

5.38. Another point of distinction between the Hiscox and Beazley business interruption clause is the omission and the inclusion of 'forensic expenses' respectively. Forensic expenses are the 'reasonable and necessary expenses incurred by the insured organization to investigate the source or the cause of the business interruption loss'.[592] Reasonable and necessary expenses is a recurring phrase however the meaning remains fluid and will be dependent on the specific facts or the circumstances and also the size of the assured. Therefore, since the ports of Liverpool have been the victim of cyber-attacks on two (2) previous occasions, what will be reasonable and necessary expenses to investigate the source of the cyber-attack may differ significantly from what another facility or a shipowner may deem necessary and reasonable and what the insurers will accept to be the same. Since the ports of Liverpool provide an essential service to a wide market with partners and customers across the world, it may be reasonable and necessary for the port authority to engage the services of a cyber risk firm rather than depending solely on their internal IT department to identify and correct the vulnerabilities within the system. Additionally, the port will be required as best practice to carry out regular penetration testing, software upgrades and staff training to maintain a cyber resilient system. The costs of the investigation along with the implementation of recommendations from the forensic report is an expense which the assured may not be able to finance out of pocket therefore the inclusion of these expenses within the business interruption loss is important to any assured whether it be a port authority or a small business operator.

5.39. Furthermore, the assured port authority will be indemnified for their extra expenses, that is 'the reasonable and necessary expenses incurred during the period of restoration to minimize, reduce or avoid income loss, over and above those expenses the insured organization would have incurred had no security breach occurred'.[593] They will be indemnified only for added expenses, in other words whatever the difference is between the expenses that would have incurred had there been no cyber-attack / business interruption and the expenses post the cyber-attack that were incurred to reduce or avoid income loss. Despite the exclusion of 'legal cost or expenses', there is no parallel exclusion of the costs to retain an expert or specialist organization to assist and lead the

[592] Beazley (n 591) Business Interruption Loss: Definition "Forensic expenses".
[593] Ibid, Business Interruption Loss: Definition "Extra Expenses".

negotiation of the ransom with the hackers, who demanded £10 million in bitcoin to decrypt the network. The decision not to pay the ransom must be assessed against the losses incurred during the additional 15 days that the port remained closed before the systems were restored. The refusal to pay the ransom resulting in the additional 15 days restoration period would qualify as an extra expense to minimize loss of income. By doing so, the port authority devised an ethical, though more time consuming method to restore their network rather than paying a criminal entity the ransom demanded. These extra expenses were reasonable and necessary for the port authority to minimize, reduce or avoid income loss as there is no guarantee even with the payment of the ransom, that the port network would have been restored to its original state. If that was the case, the port would have not only lost their income but the additional £10 million in bitcoin paid as ransom and the restoration costs. It is also a strong message to cyber criminals that the ports of Liverpool will not yield to their ransom demands and that they are prepared to restore their systems offline with their own resources. Furthermore, if the port authority were to pay, that would be motivation for the hackers to continue to target the ports' network with the expectation that they would be paid the ransom requested especially when the stakes and economic impact are higher.

5.40. On the other hand, BI loss under the Beazley Breach Response policy does not include the loss arising out of liability to any third party, legal costs or expenses, loss incurred because of unfavourable business conditions, loss of market or other consequential loss, dependent business loss or data recovery costs. Rejecting at the outset any contingent business interruption and or any cargo claims from stakeholders of the Ports of Liverpool. Some cyber insurance policies will include a clause on network interruption or network security event which is a variation of business interruption clauses.[594] In some policies the coverage provided for network interruption is limited to only targeted attack intended solely to interrupt the assured's system. By description, this excludes malwares, phishing attacks or viruses that are created without a definite target.

[594] An example of a network interruption clause can be found in RSA (n 567) policy wording. The clause provides: "Cyber Business Interruption Event means: 1. Unauthorised Access or 2) any: A) damage to the Insured's data or programs or B) systems outage, network interruption, or degradation of the Insured's network, caused by a Network Security Event, discovered and notified to the Incident Manager during the Period of Insurance."

ii. Business Interruption – Gross Profit Calculation

5.41. The preceding discussion focused on loss of income / net profit basis of calculation for business interruption, which is most popular among cyber insurance. Gradually the gross profit method of calculation (typically applied in UK property BI policies) is gaining prominence among cyber insurance policies in the UK market. In this section, the researcher will discuss how an insurer whose policy is written on a gross profit basis would respond to a claim from the Liverpool port authorities regarding the business interruption losses incurred due to the DOS attacks on site.

Business Interruption Loss means the **Insured's**

1. **Gross Profit calculated as**

(unless shown as Not Insured in the Schedule)

A) **Reduction in Turnover**

the sum produced by applying the Rate of Gross Profit to the amount by which the Turnover during the Indemnity Period falls short of the Standard Turnover **in consequence** of the Cyber Business Interruption Event; and

B) **Increase In Cost of Working calculated as**

the additional expenditure necessarily and reasonably incurred for the sole purpose of avoiding or diminishing the reduction in Turnover which but for that expenditure would have taken place during the Indemnity Period in consequence of the Cyber Business Interruption Event.

Provided that

i) the sum shall not exceed the total of the sum produced by applying the Rate of Gross Profit to the amount of the reduction thereby avoided plus 5% of the Limit of Indemnity, but not more than £250,000, whichever is the lesser; and

ii) Business Interruption Loss shall apply after the Waiting Period;[595]

The Reduction in Turnover clause (1. A) above) refers to '…Turnover in consequence of the Cyber Business Interruption Event' thereby not limiting the recoverable losses to those directly caused

[595] RSA (n 577) General Definitions - Business Interruption Loss.

by the cyber business interruption event, in this case the DOS attack at the ports of Liverpool. There is growing preference for the Gross Profit approach to calculating cyber business interruption because unlike the lack of clarity and underinsurance issues identified with Net income / Net Profit approach, the Gross Profit approach is commended for its precise method of calculation and its inclusivity of fixed and variable costs. Reproduced below is an example of a definition clause explaining the Gross profit approach to calculate business interruption:

> **Gross Profit** means the amount by which the sum of the amount of the Turnover and the amounts of the closing stock and work in progress shall exceed the sum of the amounts of the opening stock and work in progress and the amount of the Uninsured Variable Costs:
>
> 1 the amounts of the opening and closing stocks and work in progress shall be arrived at in accordance with the Insured's normal accountancy methods with due provision being made for depreciation; and
> 2 the Uninsured Variable Costs shall have the meaning usually attached to them in Your accounts.[596]

5.42. Aligning the definition of 'uninsured variable costs' to the meaning attached to them in the assured's accounts is intended to remove or at least minimize the ambiguity relating to the meaning of variable costs in the maritime sector or more specifically among ports and the meaning of the term in the wider business community. Yet, reference to 'Your accounts' still leaves room for interpretational disputes as to what will qualify as uninsured variable costs since 'the specific business accounts was not identified, that is whether it alludes to the assured's management accounts, statutory accounts or other accounts maintained by the business'.[597] Moreover, like the Loss of income / Net profit approach, there is still the risk of underinsurance 'where the Rate of Gross Profit used by the business differs from the rate of gross profit applied in the policy'.[598] As a result, it is more likely that 'the sum insured will be underestimated and the premium charged too low to cover the loss in the event of a claim, thus causing the assureds loss to be reduced.'[599]

[596] RSA (n 577) General Definitions – Gross Profit.
[597] CILA & Insurance Institute of London, 'Business Interruption Policy Wordings - Challenges Highlighted by Claims Experience' (Research Study group 265, April 2019) <https://www.cila.co.uk/cila/downloads/sig-downloads/business-interruptions/files-9/13-bi-policy-wordings/file> accessed 18 September 2022.
[598] Ibid para 6.1.2.
[599] Ibid.

c. The effect of the Trends Clause

5.43. The definition of Standard Turnover in policies written on the Gross Profit basis, includes a trends clause. An example of the definition given to Standard Turnover in a cyber business interruption provides as follows:

> **Standard Turnover or Standard Gross Revenue** means the Turnover or Gross Revenue which would have been obtained during the Indemnity Period, if the Cyber Business Interruption Event had not occurred and allowing for trends of the Business or circumstances which would have affected the Business irrespective of the Cyber Business Interruption Event occurring.[600]

Trends Clauses are incorporated in these policies to allow the trends of the business or circumstances that would have affected the business even if the DOS had not occurred to be considered when calculating the business interruption loss. The aim of the trends clause is to arrive at results that would have been achieved but for the occurrence and consequences of the insured peril. Consequently, this type of approach best represents the actual business interruption loss of the assured, reducing or eliminating the risks of underinsurance. The effect of trends clauses and how they should be interpreted was discussed in *FCA v Arch (UK) Ltd*[601] which considered and overruled *Orient Express Hotels v Assicurazioni Generali SpA***.**[602] Lord Hamblen explained as follows:

> Whilst the basic comparison between the turnover of the business in the prior period and in the indemnity period will produce a rough quantification of the lost revenue, there may be specific reasons why a higher or lower figure would be expected for the indemnity period apart from the operation of the insured peril. For example, the general trend in the business may be such as to make it likely that there would have been increased or decreased turnover during the indemnity period in any case compared with the previous year. Equally, there may be specific reasons why the turnover during the prior year was depressed, such as a strike that affected the business, or why it would be expected to have been depressed anyway during the indemnity period, such as a scheduled strike. The purpose of the trends clause is to provide for adjustments to be made to reflect "trends" or "circumstances" such as these. The aim is to achieve a more accurate figure for the insured loss than would be achieved merely by a comparison with the prior period and to seek to arrive at a figure which, consistently with the indemnity principle, is as representative of the true loss as is possible. The adjustment may

[600] RSA (n 577) General Definitions – Standard Turnover or Standard Gross Revenue.
[601] *FCA v Arch (UK)* (n 523) [297] – [312] (Lord Hamblen SCJ).
[602] [2010] Lloyd's Rep IR 531.

> work in favour of either the policyholder or the insurer, but it is meant to be in the interests of both.[603]

5.44. The insurers in *FCA v Arch (UK)* were of the opinion that the effect of the trends clause was that they were not liable to indemnify the policyholders for losses that would have occurred due to the consequences of COVID-19 and even without the operation of the insured perils. The court held that the effect of the trends clause in a loss of gross profit policy is as follows:

> trends clauses are part of the method for quantifying the loss and not to describe the scope of the indemnity. It should, if possible, be construed in line with the insuring clause so as not to take away the cover intended by the insuring clauses, otherwise the clause would be transformed into a form of exclusion.[604]

Trends clauses are not to be interpreted as requiring losses to be adjusted on the basis that if DOS attack did not occur, the results of the business, that is the operation at the port would still have been affected by other factors.[605] When applying these principles to assess how much an insurer is liable to pay the assured for their loss, "there must first be an identification of the activities which were interrupted by the insured peril. Second, identify the income generated from those activities interrupted by the insured peril during the period of interruption. Third, that amount is compared with the standard turnover and adjusted to reflect any trends or circumstances which affected those activities before the insured peril occurred or which would have affected them had the insured peril not occurred. The trends or circumstances arising out of the same originating or underlying clause as the insured peril will not be included among those for which adjustments should be made.[606] These principles were summarised by the court in its concluding remarks on trends clauses:

> …we consider that the trends clauses in issue on these appeals should be construed so that the standard turnover or gross profit derived from previous trading is adjusted only to reflect circumstances which are unconnected with the insured peril and not circumstances which are inextricably linked with the insured peril in the sense that they have the same underlying or originating cause. Such an approach ensured that the trends clause is construed consistently

[603] *FCA v Arch (UK)* (n 523) [254].
[604] The Financial Conduct Authority v Arch Insurance (UK) Ltd [2021] UKSC 1; [2021] Lloyds [260] – [262].
[605] ibid [288].
[606] ibid [283],[284].

with the insuring clause, and not so as to take away cover prima facie provided by that clause.[607]

5.45. Owing to the interconnected nature of port community networks and other IT and OT systems, a DOS attack which causes business interruption at the Ports of Liverpool will also have a cascading effect on the third-party dependent businesses along the physical and digital supply chain that rely on the efficient functioning of the ports. Insurers are aware of the risk and concerns of the assureds whose liability will extend to claims from dependent companies whose businesses have been interrupted due to the cyber-attacks at the Ports of Liverpool. To address the gap in coverage, some cyber insurers have provided cover for dependent business interruption loss otherwise known as contingent business interruption loss. The contingent business interruption policy will reimburse a company for 'lost profits and other transferrable risks due to an insurable loss suffered by one or more of its suppliers or customers'.[608] The clause usually provide that the insurer will indemnify the assured if there is interruption to his business which commences during the period of the insurance, exceeds the time excess and is caused by a dependent business suffering a security breach or cyber-attack. More specifically, the assured will be indemnified for his loss of income, increased costs of working, additional increased costs and in some policies data recovery and public relations costs resulting from the cyber-attack.[609] The drawback for an assured in the Port authorities or cargo owners position with a clause of this nature is the narrow definition often applied to 'dependent business' which in one policy is restricted to 'individuals and entities that provide the assured with outsourced business processes or information technology services'.[610]

5.46. Outsourced processes are services to support the assured's business including human resource and call centre services but do not usually include the provision of products or services

[607] The Financial Conduct Authority v Arch Insurance (UK) Ltd [2021] UKSC 1; [2021] Lloyds [287].

[608] Advisen Insurance Intelligence and Zurich, 'Contingent business interruption insurance: Does your company need it?' (2015) <https://www.zurichcanada.com/en-ca/knowledge-hub/articles/2015/05/contingent-business-interruption-insurance> accessed 25 September 2022.

[609] Hiscox (n 576).

[610] Hiscox (n 576).

as part of the supply chain.[611] In excluding products and services along the supply chain, the cargo damage, business interruption and reputational harm loss do not equate to services to support the assured business or information technology services. Likewise, stevedoring services, cargo handling and warehouse storage are expected to be categorized as services that are part of the supply chain since they are intrinsically linked and necessary for end to end supply chain operations. Another insurer in defining 'dependent business interruption loss' mentions 'dependent business loss' which excludes 'loss arising out of any liability to any third party, legal costs or expenses or loss of market or any other consequential loss.'[612] The result is, it is improbable that cargo owners or other stakeholders in the supply chain will be able to successfully rely on a similar clause under their policy. Defining dependent business narrowly by stating the type of services the parties contemplated at the inception of the insurance contracts is a mechanism to limit insurers obligation to only those individuals or organisation which specifically provide IT related services. Otherwise, the insurer could find himself liable to whole world, a long list of customers and service providers along the supply chain. There are other policies which do not explicitly provide an indemnity to the assured for dependent business interruption losses, however an expansive definition of 'assured' to include dependent business will implicitly cover this type of loss.

C. Reputation Damage from the cyber-attack: Insurance Implications

5.47. Directly linked to the business interruption claim and loss of income is the damage to the reputation of the port and the dependent businesses. As will be discussed throughout the chapters, damage arising directly or indirectly from cyber risk is not usually covered by the more general business insurance policies. The observation remains true for reputational harm insurance policies. This is another clear indication of how low cyber risk was on the agenda of insurers when they were drafting these policies. It is unimaginable or rather imprudent to draft or purchase a reputational harm policy in this age which does not include a clause on cyber risk or at the very least provides an option to purchase cyber extension. Regardless, since January 2020 Lloyds has

[611] ibid.

[612] Beazley (n 591) Insuring Agreements -Dependent business interruption.

made it compulsory[613] for all policies to state if they cover or exclude cyber risks. Unsurprisingly, exclusion of cyber risks in reputational harm policies is more commonplace. Reputation Harm / Damage Insurance covers the assured loss of profit, and the crisis management fees and costs to restore the reputation of the company following a damaging incident /cyber breach from the perspective of all its shareholders. However, it is imperative to accept that the definition and treatment of reputational harm are not uniform thus they may vary across cyber insurance policies. In this section of the discussion, the researcher will analyse the reputational risks to Liverpool ports authority following the cyber-attacks. The second part of the discussion will focus on the insurance implications and the options available to the assured in seeking adequate protection against cyber induced reputational damage. The discussion will focus on cyber risk insurance and reputational harm policies since it is without merit to discuss traditional marine policies as they do not cover reputational harm. Accordingly, an assured in the maritime sector who intends to rely on their traditional marine insurance policies will not be reimbursed for the reputational damage in consequence of a cyber-attack onboard a vessel, at offices onshore or at the ports as is the situation with the DOS at the ports of Liverpool.

a. Reputational Harm Insurance

5.48. Below is an example of the reputational harm clause and a cyber exclusion clause within Beazley's Reputational Harm Insurance policy[614]

---

[613] Lloyds, 'Providing clarity for Lloyd's customers on coverage for cyber exposures (Market Bulletin Y5258)' (4 July 2019) <https://www.lloyds.com/news-and-insights/market-communications/market-bulletins/?Query=Y5258&Filters=%5B%5D&OrderBy=&Page=1&StartDate=&EndDate=&Type=MarketBulletin&DateChanged=false&HideFields=> accessed 25 September 2022.
; Lloyds, 'Update- Providing clarity for Lloyd's customers on coverage for cyber exposures (Market Bulletin Y5277) (29 January 2020) <https://www.lloyds.com/news-and-insights/market-communications/market-bulletins/?Query=Y5277&Filters=%5B%5D&OrderBy=&Page=1&StartDate=&EndDate=&Type=MarketBulletin&DateChanged=false&HideFields=> accessed 25 September 2022.

[614] Beazley Reputational Harm Insurance Policy (nd) <https://www.beazley.com/documents/Management%20Liability/RepRisk/Beazley-executive-risk-Reputational-Risk-wording-us.pdf> accessed 25 September 2022.

A. Insuring Clauses

Reputational Harm Coverage

The insurer will pay loss and or crisis costs arising from a notification which has been made to the insurer during the policy period pursuant to C.1., provided that:

(a) the act, incident or event described in such notification gives rises to reputational harm, and
(b) the insured organization suffers a reduction in revenue, and
(c) it is established to the insurer's satisfaction that there is causal link between the reputational harm and such reduction in revenue.

B. Exclusions

The insurer will not be liable to make any payment under this policy for pre-loss crisis costs, loss or crisis costs arising from:

2. Cyber

(b) the theft, loss or unauthorized disclosure of information or data that is in the care, custody or control of the Insured Organization or a third party for whose theft, loss or unauthorized disclosure of information or data the Insured Organization is legally responsible;

(c) (i) the unauthorised access or use of the Insured Organization's computer systems;

(ii) a denial-of-service attack or any disabling action against any computer system; or

(iii) the infection of the Insured Organization's computer systems by malicious code or other malware, or transmission of malicious code or other malware, from the Insured Organization's computer systems,

whether any of the foregoing is a specifically targeted attack or a general distributed attack; or

(d) the Insured Organization's actual or alleged failure to comply with, or violation of, any law or regulation requiring the Insured Organization to protect the confidentiality and/or security of any information or data.

If the port operators were in possession of a reputational harm policy which included a clause with the same or similar wording, the policy coverage would only be triggered at the point where there is a reduction in turnover. More importantly, the burden falls on the assured to establish a causal link between the reputational harm, in this case the multiple cyber-attacks at the ports of Liverpool and the reduction in turnover following those attacks. Despite the reduction in turnover, an inability to establish the causal link means they will not be indemnified for the losses or crisis management costs arising from the DOS attacks. The exclusion clause is widely constructed in

that it considered many of the methods by which hackers and malicious persons may target an organization including denial of services or any disabling actions against any computer system which captures even ransomwares as an attack vector. If the said clause formed part of a policy that the Liverpool Port authority had at the time of the cyber-attack, the insurer would be absolved from any payment under the policy for pre-loss crisis costs, loss or crisis costs arising from the denial-of-service attack and the disabling of the Port's computer system. Moreover, the insurers did not leave any opportunity for gaps in coverage in that it not only excluded loss from targeted attacks but also specifically excluded a general distributed attack to which the port may unintentionally fall victim for example incidents of phishing, ransomwares, and malwares. The exclusion of cyber risks is a normal feature among traditional reputational harm insurance policies. Any protection against such risk must be purchased through an extension clause covering cyber risks or alternatively through a cyber insurance policy that includes a reputational harm clause, details of which will be explored below.

5.49. Fortunately for port operators and shipowners who purchase a cyber insurance policy, insurers, brokers, and assureds have on a wide scale adopted and included within these policies a reputation protection clause designed to cover public relations costs, loss of income and the additional expenses resulting solely and directly from the damage to their reputation. Some cyber policies offer reputational damage from a cyber breach as a separate cover with its own sub-limits. The challenge for the parties to the insurance contract is understanding and determining the reputational damage point of impact, the duration of reputational damage, how is damage to reputation calculated and whether future loss will be accounted for. Providing a general response to these questions is difficult as the triggers required may vary among policy providers. However, for some policies, the triggers can be either or all the following, but this will depend on the risks profile of the assured's company. The reputational damage is 'first triggered by an incident affecting the reputation of the company, secondly, the insurers will look at the media coverage and the volume of negativity published about the ports of Liverpool and third, the significant decrease in turnover'.[615] During this process and after the significant reduction in turnovers, the loss

[615] Munich Re Facultative & Corporate, 'Reputational risk insurance Covering financial loss' (2016)

adjuster's role is to determine which part of the reduction in turnover is due to the DOS incident. To decide this, all other factors that might have affected the turnover will be excluded. Finally, the gross profit margin is then applied to reduction in turnover to determine if there was indeed a drop in profit.[616]

5.50. The most immediate and noticeable impact would be reduced traffic at the port until customers and other stakeholders regain confidence in the system through public relations campaigns highlighting that safety measures have been implemented to prevent another cyber incident of this magnitude at the port. So, there may be revenue losses, loss of opportunity cost, crisis handling costs and the costs for restoration of the goodwill of the port. It is recommended that "loss of reputation due to a data breach should be defined and calculated on the same basis as business interruption losses arising from network security interruption or failure which requires repair of the system".[617] Each policy may choose a different method of calculation, either i) the formerly more popular loss of income or net income approach or ii) the increasingly popular Gross Profit approach or iii) the less popular Gross revenue Approach.[618] Celso de Azevedo proposed that the Rate of Gross Profit in the Gross Profit calculation should be 'adapted in stand-alone cyber policies so as to refer to the "network system interruption or data breach"[619].

> Rate of Gross Profit – The Rate of Gross Profit earned on the Turnover during the financial year immediately before the network system interruption or data breach

Seasonal variations will be accounted for through trends clauses by comparing the calendar period of days and months of the year preceding and the same days and months post the network interruption. If a cyber policy does not include a trends clause, 'there will be issues in correctly choosing the profit that should be used as the measuring post as to what should be expected as profit if there was no interruption to the businesses at the ports due to the DOS'.[620] Based on the

<https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/F-C_Productsheet_Reputational_Risk_Insurance.pdf> accessed 25 September 2022.

[616] ibid.

[617] de Azevedo (n 575) para 6-001.

[618] See discussion on each method of calculation above.

[619] de Azevedo (n 575) para 6-013.

[620] ibid.

definitions and the applicable principles, the formula for the calculation of the indemnity payable to the assured for a reduction in turnover is:

> Rate of Gross Profit multiplied by the sum by which the actual turnover during the indemnity period fall short is taken from the Standard turnover.
>
> Where Rate of Gross Profit = $\frac{\text{Previous financial Year Gross Profit}}{\text{Turnover}}$
>
> And Standard Turnover is the "Turnover earned during the 12 months immediately before the date of the network interruption or data breach which corresponds with the indemnity period.[621]

While the Gross Profit calculation is still new for cyber insurance policies, the result produces a more accurate representation of the losses suffered by the assured due to reputational damage from network interruption or other types of cyber-attacks for example the DOS attack at the ports of Liverpool. The main reason for this is that the Gross Profit approach provides a longer indemnity period, continuing beyond the expiration of the indemnity period to include the period during which consequential losses still affect the operations of the port but not exceeding the maximum indemnity period. Applying the Gross Profit approach will also consider ongoing fixed costs which might not be covered under a loss of income policy.

b. Public relations or crisis management consultant- re-establishing business reputation

5.51. As it relates to the public relations costs, what is covered is the reasonable costs incurred for public relations and crisis management consultants to assist the assured in re- establishing the reputation of the business. An example of this clause is described in Hiscox Cyberclear cyber and data insurance policy wording which provides:

> **Public relations costs**
>
> The reasonable costs incurred with our prior written agreement:
>
> 1 for a public relations or crisis management consultant to assist you in re-establishing your business reputation and to respond to media reports, including the development and communication of a strategy to repair your reputation;
>
> 2 to issue statements via email or your website and social media accounts, including

[621] de Azevedo (n 575) para 6-013.

managing and monitoring your social media sites; and

3 **for any other reasonable and proportionate measures** taken to protect or re-establish the reputation of your business.[622]

5.52. The inclusion of the public relations clause in CRBI policies is important to manage the reputational harm damage which may occur from the DOS attacks at the ports of Liverpool. The increasing reliance on and access to technology-increases the speed at which information is shared across social media networks and beyond international borders. Therefore, an assured will value the services of a public relation or crisis management to quickly respond to, monitor and develop communication strategies which are reasonable and proportionate to repair the reputation of the business. The essential services offered by a port facility such as the Ports of Liverpool mean that any compromise to the safety procedures will quickly attract public interest and will be aired by several news networks across the world especially because many of the supply chains and those who will be affected live, work and operate beyond the shores of the UK. Furthermore, the regulatory obligations under the Data Protection Act 2018 makes it mandatory for the port authorities to report to the ICO and to notify customers whose data may have been stolen during the attack upon the port.[623] Reputational harm is a major risk concern among corporations especially those the size of the Ports of Liverpool. The measures which the Ports of Liverpool need to implement to repair or minimize its reputational harm will not necessarily be the same response from a small and medium sized enterprise (SME) or shipowner with one or two vessels. As such, there is no one size fit all formula and the size of the corporation should have a role to play in determining what is to be accepted as 'reasonable and proportionate measures'. Other factors such as the attack vector, perpetrators and their motive and the potential scale of impact will also be considered.

5.53 The reputational impact of a crises on an organization has doubled since the advent of social media. The recurring cyber-attacks on the port will affect its reputation resulting in 'increases in the port's equity beta and the costs of capital' which is an indication to insurers and

[622] Hiscox (n 576).
[623] Data Protection Act 2018, s 68 (1).

investors that the port is a high risk.[624] In the Pentland Analytics study examining 125 reputation events over the last decade, the objective of the research was to examine the dynamic between reputation risk and shareholder value. The aftermath of each incident was studied for a year. The impact varies across companies which was divided into 2 categories 'winners' and 'losers' from both the 2000 and 2018 studies. The winners are the companies that outperform the pre-crisis expectations of investors while the losers are the companies who experience a fall in value. The winners in the 2000 gained on average 10% in value while the losers group sustained a loss of about 15% on average.[625] On the other hand, the winners in the 2018 and 2020 gained an additional 20% in shareholder value while the losers loss almost 30% of their holder value after a reputation crisis.[626] This indicates that in the 2018 study which coincides with the introduction and growing use of social media, the gain and losses from a reputation crisis doubled over a decade. Undeniably, social media played a pivotal role in the difference between the shareholder values after a reputation crisis in 2000 and those in 2018 which demonstrates as well how easy, cheap and fast news of a crisis can be circulated on social media and the immediate and long-term impact of the negative attention garnered on the various social media websites.

5.54. Another factor which may have affected the values in the 2018 study as distinct from the 2000 study is that there were 23(18%) cyber-attacks among the companies within that portfolio whereas there were no cyber-attacks in the previous study in 2010.[627] In the 2020 study, there were 30 major cyber-attacks.[628] Therefore, it is reasonable to conclude that both the use of social media and the occurrence of a cyber-attack will drastically change the shareholder value of a company that has experienced a reputation crisis. This analysis is not unique to the companies involved in the Pentland study, as such a similar outcome is expected approximately a year after the most

---

[624] Deborah Pretty, 'Reputation Risk in the Cyber Age: The Impact on Shareholder Value' (Pentland Analytics 2018) 14<https://www.aon.com/getmedia/2882e8b3-2aa0-4726-9efa-005af9176496/Aon-Pentland-Analytics-Reputation-Report-2018-07-18.pdf?utm_source=aoncom&utm_medium=storypage&utm_campaign=reprisk2018> accessed 25 September 2022.

[625] Ibid 13.

[626] Ibid; Deborah Pretty, 'Risk, Reputation and Accountability: A Governance Perspective of Disruptive Events' (Pentland Analysis, 2020), 5 <https://www.pentlandanalytics.com/wp-content/uploads/2020/09/Pentland-Analytics_Governance-paper_2020.pdf> accessed 25 September, 2025.

[627] Pretty, 'Reputation Risk in the Cyber Age (n 624) 13-15.

[628] Pretty, 'Risk, Reputation and Accountability (n 626) 6.

recent cyber-attack on the ports of Liverpool. Of course, the values will also depend on whether the port will emerge as a 'winner' or 'loser' but in any event the impact of social media and the cyber-attacks on the ports' reputation and shareholder value will be substantial. While it is difficult to calculate the precise value of reputation, research conducted on companies in the world's leading market indices showed that '35.3% of the overall market capitalization was attributable to corporate reputations which equates to $16.77 trillion of shareholder value.'[629] The same research showed the correlation between growing reputation value and stock values. Of the 1,611 companies in the study, '79% of the companies' corporate reputations led to an increase in their stock value, accounting for $17.2 trillion of the market capitalization, on the other hand 21% of the companies market cap reduced by $436 billion due to the impact of negative reputations'.[630] These values will vary across companies and geographies, however what is certain is the correlation between the reputation of an organisation and its shareholder value.

5.55. There is no mention made of the limit placed on the amount that the insurer is willing to pay for these costs, however this may not be a concern considering that the measures contemplated by the assured and the associated costs must first be approved by the insurer. An interesting question is whether the insurer agreeing to such services by a consultant company inherently means that the insurer will be paying to re-establish a reputation that was damaged prior to the commencement of the insurance between the assured and the insurer? In other words, as the facts herein dictate, the port of Liverpool had experienced two (2) cyber-attacks preceding the last incident which completely put the port out of business. This means that prior to the final incident, the reputation of the port was already at risks as confidence in the security system waned among the stakeholders and users who were aware or suspicious of the security breaches. An insurer can avoid adopting the reputational damage that existed prior to the inception of his insurance by retaining the services of a forensic accountant to determine the causal relationship between the

[629] Simon Cole, 'What price reputation?: Corporate Reputation Value Drivers: A Global report' (AMO Strategic Advisors and Reputation Dividend 2019) 6 <https://www.reputationdividend.com/files/6415/6215/6989/RD_AMO_GLOBAL_REP_VALUE_030719.pdf> accessed 9 December 2021; <https://www.australasianir.com.au/common/Uploaded%20files/AIRA%20Documents/Member%20Update%20Documents/AMO_What_Price_Reputation_report_R2[2]%20(1).pdf> accessed 25 September 2022.

[630] Ibid 8.

event which induces the reputational harm and the reduction in revenue. The insurer should also request documentary proof of the reputational harm, loss, and reduction in revenue, so trends and fluctuations are identified and matched with the lifespan of the insurers policy. Lloyds and KPMG (Klynveld Peat Marwick Goerdeler) advise assureds to develop a crisis management protocol which should include a 'signal sensing and horizon scanning' system. The purpose of such system is to 'track changes in shareholder and public sentiments about the organization and to adjust internal behaviours and predicting pathways towards the crises.'[631]

5.56. While there may be some level of reputational damage prior to the DOS attack which halted the operations at the port, considering the points discussed above relating to triggers of reputational harm insurance, it is unlikely that the insurer will be paying for damage which occurred prior to the commencement of the insurance. As aforementioned, the point of relevance in a reputational harm clause or policy is the time at which there is a recognizable reduction in the turnover or income of the assured coupled with negative media coverage and negative perception among the company's shareholders. Only then will most reputational harm clauses or policies be triggered, and it is unlikely that a new insurer will cover these losses without noticing the changes before the insurance contract is signed. It is expected that before any new cyber insurance or reputational harm policy is signed, the assured will; fairly present its risks pursuant to s.3 of the *Insurance Act 2015* and the insurers will complete penetration or other security test, audit financial and accounts statements and assess company value before they accept the risk or at the very least set the appropriate premium. The assured as a company is deemed to have the knowledge of the senior management and for the purposes of a cyber policy, it is expected that senior management will include the IT management team and security personnel. Another obstacle is that the peril which caused the reputational harm must have occurred during the operation of the current insurers policy, therefore all assessments will be based on the financial and shareholder value figures at the time of contract. So, while it is possible that the new insurer may incur some of the losses that

[631] Lloyds and KPMG. 'Safeguarding reputation: Are you prepared to protect your reputation?' (25 November 2020) 9 <https://www.lloyds.com/news-and-insights/risk-reports/library/safeguarding-reputation> accessed 25 September 2022.

should have been covered by the previous insurer, this is very unlikely based on the pre-contractual processes which are performed before a contract is agreed.

5.57. The crisis management post the cyber-attack will be the main difference in how much harm will be done to the reputation of the port. The Home Depot security breach 2014 and Talk Talk (UK) cyber-attack in 2015 are two examples of how post incident behaviour can reduce the impact of a cyber-attack or any form of security breach upon an organisation. Home Depot revealed there was a breach to its payment card systems which exposed the credit and debit card details of over 56 million customers. The estimated cost of the attack is USD 10 billion. Home Depot was quick in their response, immediately activating its incident response plan. They offered customers free credit monitoring, took the affected terminals out of service, eliminated the malware from its computers and improved their encryption technology. As a result of the swift and customer focused response by the management of Home Depot, the company was able to add over USD 30 million in shareholder value by the end of 2015, an impressive feat considering the potential for sustained reputational harm.[632] A similar incident hit home in October 2015 when Talk Talk, a UK telecommunications company was the target of a cyber-attack. Initially Talk Talk disclosed that the website was down due to technical issues, later that day they revealed they had deliberately taken the site down. The following day Talk Talk admitted that they were the target of a cyber-attack, and the next day said it was a significant sustained attack with the possibility that the personal data of over 4 million customers would be at risk. Ultimately, the result was that the personal details of 156, 959 customers was hacked, significantly lower than the suspected 4 million that was first communicated by Talk Talk. The incompleteness and inconsistencies in the communication especially on technical issues undermined the credibility of the organization despite the genuine effort of the CE0 to be visible, accept responsibility and prioritise customers. The bulk of the damage was already done in the 2 days immediately following the incident when the story was being shared and distorted over social media. During those 2 days social media ran rampant with the news.

[632] Pretty, 'Reputation Risk in the Cyber Age (n 624) 17.

5.58. This indirect response and the delayed apology of the CEO contributed to the reduction in trading revenue by over USD 20 million, Talk Talk had to book exceptional costs of between USD 60 million and USD 70 million and resulted in the loss of 101, 000 customers. By the end of 2016, one-third of the company value was taken off the shares, approximately USD 1.4 billion. This was also the third data breach that Talk Talk experienced in 2015.[633] Other events include the 2016 recall of Samsung smart phones after reports of overheating which was a fire hazard. The company first tried to replace the affected phones, but the issue continued eventually leading to a product recall. The company lost revenue of an estimated $7 billion.[634] The airplane crashes of 2019 resulted in Boeing losing a sixth of its shareholder value.[635] The public criticized the company's initial response to the accidents and its unsatisfactory safety culture.[636]

5.59. The difference in the approach of the companies illustrate the importance of an immediate and coherent response of the management and the need to have and activate their incident response plans. It is crucial that communication is open and honest, meaning the evidence matches what is being communicated. The impact of the resharing of negative or inaccurate information across the internet and on social media websites cannot be underestimated therefore considerate resources must be dedicated towards monitoring and protecting the reputation of the ports and to ultimately restore public trust in its security. The incidence of cyber and reputational risks increases with technological developments therefore the objective is not necessarily to eradicate the risks, rather it is more effective to be proactive by implementing and continuously enhancing the best practices as recommended by government, IMO, BIMCO and other specialist organisations. Likewise, it is

---

[633] ibid 16.

[634] Kate Samuelson, 'A Brief History of Samsung's Troubled Galaxy Note 7 smartphone' *Time* (New York, 11 October 2016) <https://time.com/4526350/samsung-galaxy-note-7-recall-problems-overheating-fire/> accessed 25 September 2022; BBC, 'Samsung confirms battery faults as cause of Note 7 fires' *BBC News* (London, 23 January 2017) < https://www.bbc.co.uk/news/business-38714461> accessed 25 September 2022.

[635] Lloyds and KPMG (n 631) 13.

[636] Dimitar Ganev, 'Boeing's Ethiopian Crash: A study in Bad Crisis Management' (Commetric, 12 April 2019) <https://commetric.com/2019/04/12/boeings-ethiopian-crash-a-study-in-bad-crisis-management/>accessed 25 September 2022; Sinead Baker, 'Boeing's response to the 737 Max crisis confused and frightened people, making it hard to believe apologies, expert say' (Insider, 19 May 2019) <https://www.businessinsider.com/boeing-737-max-crisis-response-confusing-hard-to-trust-experts-2019-5?r=US&IR=T> accessed 25 September 2022.

important for port managers to include within their security management considerations about reputation and cyber risk management.

5.60. Reputation is based on perception therefore any attempt to re-establish the reputation of the ports necessitates a change in public perception. It is recommended that for an organization to restore their damaged reputation, 'the organization needs to remain on the publics radar and staying above the awareness threshold by featuring in the minimum number of stories in the leading media' for example The British Broadcasting Corporation (BBC) in the UK and The Cable News Network (CNN) in the United States of America.[637] While remaining in the public's radar is important, the goal is to re-establish a positive reputation for the port therefore that means that at least 20% of the media features must be positive, no more than 10% negative and the remaining 70% can be neutral.[638] Another technique to improve the reputation of the port is to increase its 'share voice', that is increasing the leading number of media stories that quote someone from the organization or cite data that they have provided. In normal times, at least 35% management share voice is needed to keep negative perceptions to a minimum compared to the 50% management share voice needed during a crisis, a fitting description of the repeat multiple successful cyber-attacks on the Liverpool port facility.[639] The foregoing including the establishment and operation of call centres and cross border campaigns are likely to form part of the communication strategy developed to repair the reputation of the ports.

5.61. Paragraph 1 of the Public relations costs definition found in Hiscox Cyberclear- cyber and data insurance policy reproduced below, refers to 'the development and communication of a strategy to repair your reputation':

> **Public relations costs**
>
> The reasonable costs incurred with our prior written agreement:
> 1 for a public relations or crisis management consultant to assist you in re-establishing your business reputation and to respond to media reports, including the development and communication of a strategy to repair your

[637] Robert Eccles and others, 'Reputation and its Risk' (Harvard Business Review, February 2007) <https://hbr.org/2007/02/reputation-and-its-risks> accessed 25 September 2022.
[638] ibid.
[639] Eccles and others (n 637).

reputation;…[640]

A literal interpretation of the clause provides the scope for the insurer to argue they will not cover the cost to execute the communication strategy that has been developed. In other words, in terms of paragraph 1, the insurers obligation to the assured is complete upon the development and explanation of the strategy that the port will rely on to re-establish their reputation. Does communication of a strategy to re-establish the reputation of the port involve the costs associated with its execution? Would this include the cost to train staff or even the expenses to develop a new role with emphasis being on the protection and re-establishment of the reputation at the ports? Communication as used in the clause appears to be limited to transfer or sharing of information with the management or authorized personnel of the assured. If it was otherwise intended, the drafting style used in part 2 where the forms and medium of communication were clearly stated[641] would also need to be adopted in part 1. With that said, the opening phrase of part 3 which provides 'for any other reasonable and proportionate measures…'[642] widens the scope of what the insurers may be willing to cover under the public relations clause however those measures must be reasonable and proportionate to the extent and gravity of damage caused by the cyber-attacks to the ports. In addition to the public relations costs, Hiscox insurers are also willing to indemnify the Liverpool port authority for the loss of income and increased costs of working resulting solely and directly from the damage to the reputation of the assured.[643]

5.62. These are techniques which any business can implement to improve their reputation. While the Liverpool port authority has the liberty to implement any of the techniques above, the long-term effect may not be same primarily because of the essential service which the port offers. Initially, consumers and other stakeholders may be apprehensive about using the ports of Liverpool and may choose to redirect their ships and cargo to other ports especially those offering similar

[640] Hiscox (n 576).
[641] 'to issue statements via email or your website and social media accounts, including managing and monitoring your social media sites; and…'
[642] '…taken to protect or re-establish the reputation of your business.'
[643] Hiscox CyberClear, 'Cyber and data insurance Policy wording' (WD-PIP-UK-CCLEAR (1) 19029 12/18' (2018)) <https://www.hiscox.co.uk/sites/uk/files/documents/2019-03/19029-CyberClear-policy-wording.pdf > accessed 25 September 2022.

services nearby. Other customers and businesses along the supply chain may choose instead to support more local businesses thus a decrease in the demand for the services offered at the Port which eventually leads to a reduction in revenue. Nevertheless, the reputational damage and impact from the cyber-attack will be short lived mainly because of the "geographical and economic significance of ports and their removal from traditional market economy conditions where reputation correlates with business performance".[644] Though the impact may be short lived, the loss from the reputational damage is still expected to be high.

5.63. Although the public relations clause discussed seems comprehensive, the emphasis is on the role of the public relations and crisis management consultant whose main objective is to restore the reputation of the port. Yet, there is also the need for the assured port operators to have access to a forensic consultant and security specialist who will seek to identify the cause of the interruption and the person or group that is responsible for carrying out the attack. The maximum liability for this expense for example, as provided in the Tokio Marine Cyber security policy clause 1.3d should not exceed GBP 250, 000 for the expenses necessarily incurred in respect of any one claim and in total for all claims made during the period of insurance.[645] The time excess clause also applies to the reputation protection clause therefore each party to insurance contract must discuss and agree to the measures that will be applied in determining the point at which the insurer will assume responsibility for the reputation loss to the assured. The exact period will usually be stated in the schedule to the agreed policy.

D. How will the data loss and stolen cargo be treated by cyber insurers?

5.64. During the cyber-attack and after the restoration of the system, the assured discovered that the data relating to the rates, loading details, cargo number and the location of containers was wiped from the system. Further investigation confirmed that many high value containers went

[644] Lloyd's of London, Cambridge Centre for Risk Studies and Nanyang Technological University, 'Shen attack: Cyber risk in Asia Pacific ports' (2019) 55. <https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/shen-attack-cyber-risk-in-asia-pacific-ports> accessed 17 September 2022.

[645] Tokio Marine HCC, 'Professional Risks: Cyber Security Wording 0417- Public relations, forensic and security specialist services' (October 2017)<https://www.tmhcc.com/-/media/RoW/Documents/PI/Cyber/Cyber-Security-Insurance-Wording-0417.pdf> accessed 25 September 2022.

missing and have since been presumed stolen. This is unsettling to both the assured and cargo owners particularly because most cyber policies exclude loss of tangible property whereas cargo policies exclude loss from a cyber-attack. In terms of the cyber polices, examples of relevant exclusions are Beazley's Bodily Injury or Property Damage clause and 'Trading losses, loss of money & Discounts clause' which provides:

> Exclusions
>
> The coverage under this Policy will not apply to any loss arising out of:
> **Bodily Injury or Property Damage**
> 1. …
> 2. physical injury or destruction of any tangible property, including the loss of use thereof; but electronic data will not be considered tangible property
>
> **Trading losses, loss of money & Discounts**
> 1.
> 2. any loss, transfer or theft of monies, securities or tangible property of the insured or others in the care, custody or control of the insured organization.[646]

With this clause in their policy, the assured and cargo owners have no option but to settle the cost of the losses on their own without the assistance of their cyber and cargo insurers. The positive here is that the clause on property damage clarifies that 'data' is not considered tangible property therefore it does not fall within the exclusion. Accordingly, the cyber insurer will not indemnify the assured for damage or loss of the cargo but will indemnify the assured port authority for its data recovery costs, that is 'the reasonable and necessary costs incurred to regain access to, replace or restore data or if as in this case where the data cannot be reasonably be accessed, replaced or restored, then the reasonable costs incurred by the port authority to reach this determination'[647] with the assistance of the expert company hired to resolve this issue.

5.65. Hiscox Property- Business Interruption (Technology) policy wording[648] seeks to combine elements of property, business interruption and cyber risk insurance to provide the assured with a comprehensive policy option. If the Liverpool port authority had this policy at the

[646] Beazley (n 585) Exclusions.
[647] Beazley (n 585) Exclusions.
[648] Hiscox, 'Property -business interruption (technology)' (WD-TEC-UK-PYI (4) (16101 06/20)) <https://www.hiscox.co.uk/sites/uk/files/documents/2020-05/16101%20WD-TEC-UK-PYI%284%29.pdf > accessed 25 September 2022.

time of the cyber-attack, some of the gaps mentioned above as it relates to cargo loss would have been covered. The definition of a cyber-attack according to the named policy includes 'an attack by a third party who specifically targets the port system by maliciously blocking electronical access to the website, intranet, network, computer system, programmes or data held electronically by you or on your behalf'. This definition is wide enough to include the denial-of-service attack on the computer systems at the ports of Liverpool.

Hiscox Property – Business Interruption (Technology) Policy wording

> **What is covered**
>
> **We** will insure **you** for **your** financial losses and other items specified in the schedule, resulting solely and directly from an interruption to **your activities** caused by:
>
> Financial losses from insured damage
>
> 1. **insured damage to property**:
>
> a. insured under any property section of this **policy** other than equipment breakdown: or
>
> a. insured elsewhere, but not under this **policy**, provided the **damage** occurred while the **property** was contained in the **insured premises**;[649]

5.66. Under 'What is covered' section, clause 1 on financial losses from insured damage (reproduced above) and its application to the scenario, the insurer agrees to pay for the financial losses resulting solely and directly from an interruption to the port operations from insured damage to property other than equipment breakdown.[650] Indemnification for the cargo damaged while contained in the insured premises will be permitted if there was a separate property / cargo insurance in force at the time of the damage and payment has been made or liability admitted under that property / cargo insurance. Importantly, the cargo does not have to be owned by the assured, indemnification will be provided even if the assured is only legally responsible for it, for example, if he is a bailee of the property while in storage.[651] Insured damage is defined in the policy as

[649] ibid.
[650] Hiscox, 'Property -business interruption (technology)' (n 648) Special definitions for this section – Insured damage.
[651] ibid. See clause under Your obligations – Property Insurance: 'Where the damage involves property you own or are legally responsible for, we will not make any payment unless you have property insurance in force covering the damage and payment has been made, or liability admitted, under that insurance for the damage.'

'damage, other than failure, to property occurring during the period of insurance provided that the damage is not otherwise excluded by the buildings, contents or property section of the policy".[652] If 'insured damage to property' includes loss or property stolen, the insurer is liable to indemnify the assured provided other conditions within the policy are met. However, if the parties had intended to cover not just damage but also loss of property, it would have been expressly provided, for example by the inclusion of the phrase 'insured damage or loss to property' which is the approach adopted in the policy under the 'what is covered section', clauses 5 and 7 relating to unspecified customers[653] and unspecified suppliers[654] respectively. In the absence of the word 'loss' in clause 1b, it is reasonable to conclude that the parties only intended to cover damage of the property. Damage means that the property is still in existence but there has been impairment to its physical state and commercial value[655] while loss of property means the item is permanently irretrievable. In marine insurance, loss means the subject matter is destroyed or the assured is irretrievably deprived thereof[656] or unlikely to be recovered[657]. Justice Asher made a similar point in the Court of Appeal of New Zealand when the distinction was made between "damage" and "loss". He agreed that damage took its ordinary meaning of harm to something which affects its value whilst loss has a broader meaning, deprivation of something.[658] A relevant observation made by Sir Martin Nourse is that the meaning of the word "loss" will vary with the context in which it

[652] Hiscox, 'Property -business interruption (technology)' (n 648) Special definitions for this section – Insured damage and Insured failure. Insured failure includes "failure of equipment, computers, oil or water storage tanks and other insured items … provided the failure is not otherwise excluded by the equipment breakdown section of the policy…"

[653]Hiscox, 'Property -business interruption (technology)' (n 648) See clause under What is covered – Unspecified customers: insured damage, other than loss or damage caused by flood or earth movement, arising at the premises of any of your direct customers operating and based in the European Union (including in the United Kingdom or Gibraltar), other than any specified customer.

[654] Hiscox, 'Property -business interruption (technology)' (n 648) See clause under What is covered – Unspecified suppliers: insured damage, other than loss or damage caused by flood or earth movement, arising at the premises of any of your suppliers operating and based in the European Union (including in the United Kingdom or Gibraltar), other than any specified supplier. This does not apply to any supplier of water, gas, electricity or telecommunications services.

[655] *Promet Engineering (Singapore) Pte Ltd v Sturge (The Nukila)* [1997] 2 Lloyd's Rep 146, 151; *TKC London Ltd v Allianz Insurance PLC* [2020] EWHC 2710 (Comm)[26]; [2020] Lloyd's Rep. IR 63.

[656] Marine Insurance Act 1906, s. 57 (1).

[657] Marine Insurance Act 1906, 60 (2).

[658] *Kraal and Another v The Earthquake Commission and Another* [2015] NZCA 13; [2015] Lloyd's Rep. IR 379 [37]-[38].

is used"[659] In applying this observation, Richard Salter QC in *TKC London Ltd v Allianz Insurance Plc*, said that in the definition of "Event" in BI section of the policy the word "loss" appears within the phrase "accidental loss or destruction of or damage to property". As used in that context, "loss" was intended to have a physical aspect and the expression "loss… of… property" could not sensibly be interpreted as including mere temporary loss of property."[660] However, the assured does not need to establish complete deprivation amounting to certainty that the goods could never be recovered. **[661]**

5.67. Damage as used in the context of the policy even if it extends to loss of the cargo, would not extend to theft of the cargo notwithstanding it has resulted in financial losses to the assured because the theft, that is the insured damage should be the cause of the interruption to the business. This is not the case; the theft of cargo did not cause business interruption at the port. Even if the insurers were to accept the loss of the cargo as insured damage, it is a condition precedent that at the time of the damage, the assured had property insurance in force and payment has been made or liability admitted under the property insurance for damage.

a. Cargo loss from cyber-attack – Response of cargo insurers?

5.68. We will assume for the purposes of the discussion in this subsection that the cargo insurance is written on Institute Cargo Clauses A (ICC (A) 1/1/09[662] and will make comparisons

---

[659] Tektrol Ltd v International Insurance Co of Hanover Ltd [2005] 2 Lloyd's Rep 701; [2006] Lloyd's Rep IP 38 [27]; *Pilkington United Kingdom Ltd v CGU Insurance plc* [2004] Lloyd's Rep IR 891, 50.

[660] *TKC London* (n 655) [124], [128].

[661] *Moore v Evans* [1918] AC 185. Pearls were sent abroad for sale but should be returned if the sale was unsuccessful. World War I broke out which meant that the jeweller was unable to retrieve his jewellery at the time. The court held that there was no evidence that the Germans seized the pearls, the Jewellers would just have to wait many years to retrieve them and on that basis the jewellery was not 'loss'. Compare with *Scott v The Copenhagen Reinsurance Co* (UK) Ltd [2003] Lloyds Rep IR 696 where a Kuwait Airways aircraft and a British Airways aircraft was captured during Iraq's invasion of Kuwait. Iraq intention to capture both the airport and the aircraft is strong evidence that the Kuwait aircraft should be treated as a 'loss'. Conversely, the claim for the loss of the British Airways aircraft was rejected since the capture or detainment was deemed temporary as there was a realistic prospect of recovery.

[662] Lloyds Market Association and International Underwriting Association, 'Institute Cargo Clauses (A)' (CL382 1/1/2009) <https://www.lmalloyds.com/lma/underwriting/marine/JCC/JCC_Clauses_Project/Revised_Clauses/ICC_A_CL382.aspx> accessed 25 September 2022.

where relevant with ICC (A) 1/1/82[663]. Loss from a piracy event is an insured peril under ICC (A); it is not one of the excluded perils.[664] There is no exclusion or endorsement of cyber risks in the unamended version of either ICC (A) 1/1/82 or 1/1/09. Each cargo interest may purchase a cyber extension cover under their cargo or property damage insurance, the limitations of which will depend on the specific words of the clause and the insurance policies. As such the analysis which follows will look at the possible responses of insurers when particular cyber clauses are attached to the traditional cargo policy of the assured cargo interest.

The Cyber Coverage Clause (JC2019-004)[665] was designed for use in the cargo market. Paragraph 1.1 of the clause imposes a condition on the insured to demonstrate that they have 'exercised due diligence and to an objective standard implemented reasonable measures in compliance with the recommendations of the UK National Cybersecurity Centre (NCSC)[666] or other equivalent organisation that was current at the inception of the policy.' If this condition is met, the insurers will indemnify the assured for any physical loss or damage, liability or expense that would normally be covered under the policy, which affects solely the insured or the insureds property and arises from the use of software[667]. This is an issue because there have been multiple security breaches at the Ports of Liverpool including the fact that the port network was still being operated on an outdated system. These are evidence to support the point that the port authority was not in compliance with the recommendations NCSC[668] and other regulatory and industry guidelines on maritime cyber risks management[669].

---

[663] Institute of London Underwriters, ' Institute Cargo Clauses (A) (CL252 1/1/82)
< https://iua.co.uk/IUA_Member/Clauses/eLibrary/Clauses_Search_Title.aspx?SUB=MIC> accessed 25 September 2022.

[664] ICC (A) 1/1/82, Clause 6.2 and ICC (A) 1/1/09, Clause 6.2.

[665] IUA, 'Cyber Coverage Clause' (JC2019-004, 18/07/2019)
< https://iua.co.uk/IUA_Member/Clauses/eLibrary/Clauses_Search_Title.aspx?SUB=MJCC> accessed 25 September 2022.

[666] The role of the UK NCSC critical organisations in the UK, the public and SME with digital risks and provide incident response to minimise harm to the UK, help with recovery and issue practical guidance on cybersecurity.

[667] JC2019-004, para 1.2. Software means programs, source codes, scripts, applications and other operating information used to instruct computers to perform.

[668] NCSC, 'Denial of Service (DoS) guidance' (Version 1, 20 January 2019 revised 19 November 2020)
< https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection> accessed 25 September 2022.

[669] IMO, 'Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.1)' (14 June 2021)

5.69. However, the assured will not be indemnified for the physical loss, damage, liability or expense arising from software which leads to a systemic loss, except where the cargo / insured property is onboard a conveyance. Conveyance would suggest for example being onboard a lorry or vessel or other means of transport but not while being held in a storage area at port or in a contractor's warehouse. If the insurance incorporated ICC (A) 2009, a conflict would arise since there is inconsistency between paragraph 1.3 of JC2019- 004 and clause 8 of ICC (A) 2009 in that cover under the latter commences when the property is 'first moved in the warehouse or at the place of storage for the purpose of the immediate loading into or onto the carrying vehicle or other conveyance for commencement of the transit'. Whereas para 1.3 of JC2019- 004 will not cover physical loss caused by software unless the damage occurred onboard any means of conveyance. Unlike ICCA 2009, there is no prerequisite in JC2019-004 for the insured property to be moved for immediate loading and for the purpose of the commencement of the insured voyage. This suggest that even if the cargo is loaded on a conveyance and sitting in the warehouse, the cargo insurers will be liable to indemnify the assured for his loss even if the assured and his property are not the only victims of the cyber-attack. That result will be in stark contrast to the intended outcome under ICC (A) 2009. An insurance policy incorporating both ICC (A) 2009 and JC2019-004 may cause interpretation issues. Since JC2019-004 was added to specifically address cyber risks, it would operate in that limited sphere so that for cyber related loss, the insurer will not be expected to indemnify the cargo owners for property loss or damaged while being moved in the warehouse for immediate transit notwithstanding the ICC (A) commencement clause. If such interpretation is accepted there would be two different commencement regimes operating under one (1) policy; a cyber related and non cyber related regime but JC2019-004 would take precedence as the bespoke clause.[670] In any event, that may not have been the intended result, thus it is important that parties ensure that the language of the endorsements clause matches that contained in the original policy.

<https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf> accessed 25 September 2022.

[670] *Hombourg Houtimport BV (Owners of cargo lately laden on board the ship or vessel "Starsin") and others v Agrosin Private Ltd (Owners and / or demise charterers of the Ship or vessel "Starsin") and others* [2003] UKHL 12; [2003] 1 Lloyd's Rep 571. Lord Bingham "… it is common sense that greater weight should attach to terms which the particular contracting parties have chosen to include than to pre-printed terms probably devised to cover very many situations to which the particular contracting parties have never addressed their minds." [para 11].

This ‘conflict’ would not arise under ICC (A) 1/1/82 clause since cover commences ‘from the time the goods leave the warehouse or place of storage and at that point must have been on some means of conveyance thus any damage or loss of property while being transported on the conveyance would have satisfied the terms of the clause.

5.70. A problematic element of JC2019-004 is the insurers refusal to indemnify the assured for physical loss or damage where others have been affected by the same incident. This is the effect of paragraph 1.2 where the words ‘affects solely the insured or the insured’s property’ appears reinforced by paragraph 1.3 definition and exclusion of systemic loss, that is loss otherwise recoverable, but which affects a third person or the property of anyone other than the assured. Paragraph 1.4 limits the liability allowed for each and every loss or series of loses arising out of one event and annual aggregate, the amount specified to be agreed by the parties. That is one of the techniques employed by the insurers to manage their risks. Since the loss of cargo at the port of Liverpool would have affected multiple cargo owners, carriers and the bill of lading holders, the insurance implication if the JC2019-004 clause was added to a traditional cargo policy is that the assured would not be indemnified by insurer because there is systemic loss at the port. If the cargo / containers were onboard a vessel or other means of conveyance the results would have been different since insurers would be prepared to indemnify the assured notwithstanding the loss to others or their property on the conveyance. The reason for the difference in approach is the insurer’s need to guard against aggregated or wide scale loss, the idea being that the loss onboard a conveyance is more contained in comparison to accepting liability for all the loss from software at the ports of Liverpool. If some of the containers were loaded onto a lorry and others sitting in a warehouse at the port, applying the terms of the clause would mean that the owners of the damaged or loss cargo that was being held in the warehouse would not be able to recover for their loss while owners whose cargo was loaded on the lorry could recover for the loss or damage to the cargo. This is a somewhat bizarre result, but it is also the literal meaning of the clause.

5.71. Another cyber endorsement clause which could be attached to a traditional cargo policy is JC2020-014 (Marine Cargo Cyber Exclusion and Affirmation Endorsement).[671] Paragraph 1 is a repeat of paragraph 1 of CL.380 effectively excluding loss, damage, liability or expense indirectly .or directly caused by or contributed to by or arising from the use or operation as a means of inflicting harm any computer system, software program, malicious code, virus, computer process or any other electronic system. Paragraph 3 provides that if JC2020-014 is endorsed on policies covering war risks, terrorism, or political motive the exclusion would not apply to losses that would otherwise be covered arising from the use of computers, computer system etc. Yet in paragraph 2, there is an affirmation of cover for loss from the use or operation of any computer, computer system, software, programme, computer process or other electronic system if such use or operation is not used or operated as a means for inflicting harm. The exclusion in paragraph 1 would apply to the facts of the current scenario so that cargo policy holders would not be compensated by insurers for their loss because the DOS attack was used as means of inflicting harm on the ports of Liverpool.

5.72. Alternatively, for an additional premium the cargo owners or bill of lading holders can attach CL.437 to their cargo policy. CL.437 (Cyber Exclusion and Write-back Clause)[672] is a write back of CL.380 and operates as a paramount clause thereby overriding anything inconsistent therewith, except the Institute War Clauses. In effect, whereas paragraph 1 of the clause excludes both non malicious and malicious loss, damage or liability caused by, contributed to or arising from any computer system, software programme, code or process or any other electronic system; paragraph 2 provides that the exclusion in paragraph 1 will not apply to physical damage or loss, general average or salvage charges where directly caused by a list of named perils[673] including

[671] IUA, 'Marine Cargo Cyber Exclusion and Affirmation Endorsement' (JC2020-014, 29 June 2020) <https://www.iua.co.uk/IUA_Member/Clauses/IUA_Member/Clauses/eLibrary/Clauses.aspx?hkey=6f7dd1a3-6ab3-4b10-94c2-5a8c644b1c32> accessed 25 September 2022.

[672] JCC, 'Cyber Exclusion and Write-back Clause' (CL.437, 18/11/2019) < https://www.lmalloyds.com/LMA/Underwriting/Marine/JCC/JCC_Clauses_and_Circulars.aspx> accessed 25 September 2022.

[673]In consideration of an additional premium and subject to any deductibles contained within the Policy of which this insurance attaches, paragraph 1 will not apply to physical loss or physical damage, general average or salvage charges covered elsewhere in this insurance where directly caused by or arising from one or more of the perils listed

general average sacrifice and (g) theft where the named peril results from the failure, error or malfunction or the use or operation, as a means for inflicting harm of any computer system, software programme, code or malicious code, computer virus or process or any other electronic system. An assured who holds a cargo policy with CL.437 endorsed on it will be indemnified for their theft of cargo based on paragraph 2(g) of the clause which covers physical damage or loss directly caused by theft caused by the use of the computer for inflicting harm. If the loss or damage to the cargo was not caused by one (1) of the named perils in paragraph 2, CL.437 would not have assisted the assured in his claim to be indemnified for their loss. Further, there is a focus on the direct physical damage or loss, general average or salvage charges thereby implying that indirect nonphysical losses would not be covered by insurers on whose policy CL.347 is attached. This means that claims for loss of profit or contractual liabilities and business interruption losses of dependent businesses along the supply chain would not be recoverable as they were the indirect nonphysical result of the DOS attack and theft but does qualify under the excepted conditions of paragraph 2 of CL.347.

5.73. The Joint Specie Committee produced a Cyber Attack Exclusion Clause and Write-Back (JS2018-001) and Cyber Exclusion (Targeted Cyber Attack Write-Back) (JS2019-005)[674] which if endorsed on a traditional marine insurance policy would cover physical loss or damage if the insured was able to establish it was the result of a targeted cyber-attack[675]. A failure, error, malfunction or accidental use of a computer system or programme that causes physical loss or damage would not qualify as a targeted attack. Instead, the assured must establish that the computer systems, software programme, malicious code was used to inflict harm solely on the insured or upon the insured property. The cargo owners, ship owners and port authority will not be able to

below: (a) fire or explosion (b) vessel or craft being stranded grounded sunk or capsized (c) overturning or derailment of land conveyance (d) collision or contact of vessel craft or conveyance with an external object (e) general average sacrifice (f) jettison (g) theft.

[674] JS2018-001 (10 January 2018) and JS2019-005 (22 November 2019) <https://www.iua.co.uk/IUA_Member/Clauses/eLibrary/Clauses_Search_Title.aspx?SUB=MJSC> accessed 25 September 2022.

[675] Ibid JS2018-001, Clause 1.3. "Targeted Cyber Attack means 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 where the motive is to inflict harm solely on (or upon) the Insured or the Insured's property."

rely on neither JS2018-001 nor JS2019-005 because of their inability to each prove the motive was to inflict harm solely on them or upon their property. It could be argued that all is required of the insured is to establish that the motive was to solely inflict harm on him or upon his property, therefore even if others or their property was damaged or lost in the process, that fact on its own should not derail their case that they were the sole targets of the attack.

5.74. Another clause produced by the Joint Specie Committee is the Limited Cyber Coverage Clause (Targeted Cyber Attack Write-Back) (JS2019-006).[676] Paragraph 1 excludes cover for loss, damage, expense or liability where the computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system was used or operated as a means to inflict harm. Paragraph 2 provides that subject to the terms and conditions of the policy, the insurers agree to cover physical loss or damage to the insured property if the computer was not used or operated as a means for inflicting harm. The exclusion in paragraph 1 shall not apply in two circumstances; i) where the clause is endorsed on policies covering risks of war, civil war, rebellion… terrorism or any person acting from a political motive and the loss which would otherwise be covered arises from the use of any computer, computer systems inter alia in the launch and or guidance system and or firing mechanism of any tangible weapon or missile (paragraph 3) and ii) to physical loss or damage to the property insured that would normally be covered if the assured can establish that such loss or damage was caused by a targeted cyber-attack[677] (paragraph 4). As per paragraph 6 of both JS2019 -005 and JSC2019 – 006, 'electronic data is not to be treated as property except where expressly stated elsewhere in the policy'. The problem for assureds with having any of these clauses endorsed on their cargo policy is the burden to establish that they were the sole targets of the cyber-attack and determining the effect of the clauses with focus on physical loss, damage or liability.

These requirements restrict the effectiveness of the clause in protecting the assured against cyber risks especially because it is very rare that a cyber-attack will only impact the sole target of the

[676] JS2019-006 (22 November 2019).
< https://www.iua.co.uk/IUA_Member/Clauses/eLibrary/Clauses_Search_Title.aspx?SUB=MJSC> accessed 25 September 2022.
[677] See (n 675) for the definition of Targeted Cyber Attack which is the same as paragraph 4 of JS2019-006.

attack. Moreover, it is difficult for assureds to ascertain the true targets of a cyber-attack as it may be an expensive and arduous task especially for SME. Equally uncertain is whether damage or loss to dependent third parties would prevent the assured from discharging his burden of establishing that he was the sole target of the cyber-attack, despite the evidence to support his claim. In other words, would the physical loss of cargo belonging to third party cargo owners be evidence to support a claim that the ports of Liverpool were not the sole target of the cyber-attack in scenario 4? Ultimately, cargo owners may not be able recover from their insurers if either clause was added to their cargo policy since the insurers may rely on the defence that the cargo owners were not the sole target of the attack. With the focus on physical loss, damage, liability, or expense of the insured's property, it is uncertain whether liability and expenses must be related to the physical state of the property, or it is wide enough to include delay and other nonphysical expenses and liabilities.

b. Equipment Repair – Betterment Clause

5.75. Following the security breach at the ports of Liverpool, it is immediately noted that important cargo data was destroyed.[678] Since the port network was encrypted and the hackers refused to unlock the system when the ransom was denied, it is expected that there will be damage to some of the communications and navigational equipment onboard the vessel. The issue here is understanding how the cyber insurers will treat claims for repairs / replacement of equipment or computer hardware and software after a cyber-attack. The general principle is that insurers will indemnify assureds for their loss and no more; the assured is not to make a profit.[679] If the assured is placed in a better position, a deduction must be made proportionate to the improved value of subject matter prior to its loss or damage.[680] In marine insurance, the principle is expressed in s.69(1) of the MIA 1906 regarding ship repairs where the appropriate measure of indemnity is the reasonable costs of repairs, 'less customary deductions' equivalent to one-third deduction for

[678] The insurance implications of a data breach caused by or arising from a cyber-attack is discussed in scenario 3.
[679] *British Westinghouse Co v Underground Electric Railways Company of London Ltd* [1912] AC 673; *St Albans City and District Council v International Computers Ltd* [1996] 4 All ER 481, CA; *The Golden Strait Corp v Nippon Yusen Kubishika Kaisha ('The Golden Victory')* [2007] UKHL 12, [2007] 2 AC 353 and *Omak Maritime Ltd v Mamola Challenger Shipping Co* [2010] EWHC 2026 (Comm), [2011] 2 All ER (Comm) 155.
[680] *Reynolds v Phoenix* [1978] 2 Lloyds Rep 440, 453.

betterment. However, the practice of deduction has been replaced by New for Old principle found in clause 16 of the International Hull Clauses 01/11/03 which provides that 'claims recoverable under this insurance shall be payable without deduction on the basis of new for old'. For nonmarine insurance, the cases do not have such clear margins of deduction as was customary in marine insurance neither they do all accept the new for old principle.

5.76. The legal discussion on the principle of 'betterment' in insurance law is usually related to the damage or destruction of property with the burden on the defendant insurer to establish betterment.[681] Lord Leggatt in *Endurance Corporate Capital Limited v Sartex Quilts & Textiles Ltd* made a distinction between what he describes as the 'different senses' of betterment. The first arises when the assured seeks to make improvement to property at additional cost rather than reinstate the property substantially to the state it was in before it was damaged or destroyed. The additional cost would not be recoverable unless the parties have expressly agreed to such provision.[682] Second, where the assured does not choose to improve the property but there is incidental benefit to him after the reinstatement. This occurs for example where more modern material is issued which costs less and is more energy efficient or where a machine must be replaced but the old model is no longer available. Even though there were additional costs to purchase the new vehicle, this was unavoidable therefore would not be accepted as betterment.[683] In other words repairs or replacement of software, data or navigational equipment so they have a longer life span or more modern with additional technological features is not reason for a deduction for betterment.[684] In fact, the speed at which technology and software upgrades means that it will be commercially foolhardy or even impossible to replace the data, software or computer equipment with the models previously installed on the system so there will be elements of new for old.[685] A

[681] *Pegler Ltd v Wang (UK) Ltd* [2000] All ER (D) 260, [246] citing *Oswald v Countrywide Surveyors Ltd* (1996) 50 Con L.R. 1, 6 and *Skandia Property (UK) Ltd v Thames Water Utilities* (1997) 57 Con. L.R. 65, 80.

[682] *Endurance Corporate Capital Limited v Sartex Quilts & Textiles Ltd* [2020] EWCA Civ 308 [90]; *Tonkin v UK Insurance Ltd* [2006] EWHC 1120 (TCC); [2006] 2 All ER (Comm) 550. HHJ Coulson QC held that the costs to insulate the main roof of a barn and add double glazed windows that were not part of the original property were found to be betterment, accordingly the additional costs excluded from the award to the assured [paras 357-358 and 361 and 363].

[683] *Endurance Corporate Capital Limited v Sartex Quilts & Textiles Ltd* [2020] EWCA Civ 308, para 91-92.

[684] *Harbutt's Plasticine v Wayne* Tankship [1970] 1 QB 447, 473.

[685] *Pegler Ltd v Wang (UK) Ltd* [2000] All ER (D) 260, para 243, 249.

further distinction must be made between pecuniary and nonpecuniary benefits to the assured. The general principle is that deduction should be made for the money the assured will save or reasonably expected to save from getting an improved building / property.[686] The rationale is that the financial benefit would reduce the amount necessary to put the assured back to the position he would have been if there was no damage to his property. Where the benefit to the assured is nonpecuniary, it would be unjust to make deductions for betterment because the assured did not benefit in coin / money terms nor did they choose the advantage.[687]

5.77. In *Pegler Ltd v Wang (UK) Ltd*[688], the claimant Pegler Ltd on the advice of their IT consultants replaced the computer software that the Defendants Wang (UK) Ltd initially installed in partial fulfilment of a contract between them. As part of their claim for repudiatory breach of contract, the Claimants requested in damages the fees for the replacement system inter alia. The Defendants were of the view there was betterment because of the additional features (Euro compliance, better EDI, back flushing, ability to work with Pegler's NWOW and ecommerce para 240) which the Defendants had not promised to provide. Therefore, the issue is whether allowance should be made for betterment? In response to arguments that deductions should be made for betterment when a replacement software was purchased by the Claimants on the advice of their IT consultants, the HHJ Bowsher reasoned:

> It follows from Dr. Worden's evidence that Pegler could not have bought TROPOS more cheaply by omitting those features which he says are betterment because "they are usually not separable from the cost of the main TROPOS product". If Pegler could have bought a package omitting the alleged "betterment" features, it would have been possible (if the case on betterment were accepted) to compare the price of TROPOS as bought with the price of TROPOS without the alleged betterment features and deduct the difference from the damages. An alternative approach might have been to compare TROPOS with other systems on the market without the alleged betterment features. Neither Dr. Worden nor any other witness sought to identify another cheaper product which did not contain

[686] *British Westinghouse Co v Underground Electric Railways Company of London Ltd* [1912] AC 673. In this case the House of Lords held that the savings to the railway company when steam turbines were purchased to replace less efficient ones supplied by the appellants should be considered when assessing the damages for the breach of contract.

[687] *Harbutt's 'Plasticines' Ltd v Wayne Tank & Pump Co Ltd* [1970] 1 QB 477. The plaintiff factory was destroyed by fire caused by the installation of faulty equipment by the defendants. The plaintiff rebuilt the factory without intentional improvements and the Defendants did not prove there was savings to the plaintiff as a result. The Court of Appeal held that the plaintiffs were to be compensated for all the building costs without deductions to reflect the benefit of getting a new factory.

[688] *Pegler Ltd v Wang (UK) Ltd* [2000] All ER (D) 260.

> those features. If he had done so, it would have both been possible to put a precise figure on the sum which, according to Wang, ought to have been saved and to investigate whether Pegler ought reasonably to have bought that other system. There is no evidence that SSI were able to raise the price of TROPOS above the cost of competing products because of the alleged betterment features other than Dr. Worden's bland assertion.[689]
>
> … Whilst TROPOS is superior to FACT, the additional functionality is 'standard' in a medium package in today's market. The scope of the identified betterment is due primarily to current market requirements which are taken account of in most modern systems".[690]

5.78. If the Port authority find it necessary to retain the services of a consultant after the cyber-attack, they ought to first request the permission of their insurer who if agree, will cover the reasonable costs for a suitably qualified consultant to review the electronic security and the reasonable costs of any electronic security improvements as recommended by the consultant. Agreeing to cover the costs associated with improving the electronic security at the port is one of the benefits of **Hiscox Property -Business (Technology)**. Most insurers will only indemnify the assured for the cost to restore their security system to the level it was before the incident, rarely will they cover improvements above the state the system was in at the inception of the policy. An example of this is the Betterment Clause found under the General Exclusions of **Tokio Marine Cyber Security Wording 0417** which provides:

> **General Exclusions**
>
> The insurer shall not be liable to indemnify the Insured against any Claim, Loss, liability, costs or Defence costs and expenses:
>
> **Betterment**
>
> For repairing, replacing or restoring the Insured's Computer System to a level beyond that which existed prior to any Claim or Loss;[691]

There are other betterment clauses which are more in line with the decisions in Endurance and Pegler Ltd where exceptions are made for improvement / betterment when it is necessary to end a material interruption or computer component damaged cannot be repaired or

---

[689] Ibid [245].

[690] *Pegler Ltd v Wang (UK) Ltd* [2000] All ER (D) 260, para 250.

[691] Tokio Marine HCC, 'Professional Risks: Cyber Security Wording 0417- General Exclusions Betterment' (October 2017) <https://www.tmhcc.com/-/media/RoW/Documents/PI/Cyber/Cyber-Security-Insurance-Wording-0417.pdf> accessed 25 September 2022.

replaced due to unavailability of the previous model or it is simply cheaper. Thus, replacement necessary for the computer system to operate must be substituted with an upgraded version or a software. An example of this clause is the betterment exclusion below:

> Betterment
>
> Consisting of the costs of:
>
> (i) updating, upgrading, enhancing or replacing any component of a Company Computer System or an OSP Computer System to a level beyond that which existed prior to the occurrence of a Material Interruption: however, this exclusion shall not apply to the extent that the replacement of a component of a Company Computer System is:
>
> (a) required to end the Material Interruption; and
>
> (b) no longer available and can only be reasonably replaced with an upgraded or enhanced version; or
> (ii) removing software program errors or vulnerabilities[692]

5.79. Moreover, the maintenance of good cyber security practices are encouraged and the assured must implement measures to protect the computer system and networks, regularly backup all electronic data and to keep copies away from the location where electronic data is normally held. Once the assured port authority can demonstrate they took these reasonable steps, the insurer will pay for what is covered under the clause on cyber-attack. This is an issue for the assured as the facts reveal that one of the main reasons for the cyber-attack was the vulnerabilities within the ports computer system exposed through operating on an outdated Windows 7 which cannot be patched or updated. The insurers can depend on this negligent omission or failure on the part of the assured to deny the claim and or rely on an exclusion clause on outdated systems. A defence of this nature was relied on by the insurers in *Columbia Casualty Company v Cottage Health System,*[693] where the court decided that the data breach was caused by Cottage's failure to continuously check and maintain security patches, reassess information security exposure, implement security procedures and risk controls and as such Columbia was not obligated to

[692] AIG, 'CyberEdge Coverage Policy Tour' (GBL00003622, n.d) https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Financial-lines/Cyber/cyber-policy-tour.pdf accessed 25 September 2022.
[693] *Columbia Casualty Co. v. Cottage Health System*, 2:15-cv-03432 (C.D. Cal. May. 7, 2015).

indemnify or defend Cottage for the claims or potential damages.[694] Though this was a decision of the US District Court, Ninth Circuit California and therefore not binding on courts in the UK, the case is a clear indication of the mindset of insurers and their willingness to reject a claim based on an express exclusion clause for 'failure to follow minimum required practices'. It is the researcher's view that even without an express exclusion clause, there will be an implied clause of the same nature in cyber insurance policies with the same effect if the assured has also failed to exercise due diligence to follow minimum industry standards or those expressed in their application for the policy. In fact, there are policies in the UK for example Tokio Marine cyber security policy wording 0417, general conditions 8 a and b which list having virus protection software operating, correctly configured and regularly or automatically updated and updating computer systems with new protection patches issued by the original system or software manufacturer of supplier as reasonable steps an assured should take to protect its computer systems and avoid loss.[695]

E. The potential for aggregation of losses

a. Disruption and losses along the Supply Chain Loss

5.80. Enisa Report on port security has identified some of the cybersecurity challenges which supply chain that ports are associated with may experience. These include 'lack of cybersecurity certifications for port products and services, risks associated with a supplier's remote access to the port's network / system, long patching cycles for some systems for example industrial control systems and contractors lack of control over the cybersecurity levels of their suppliers.'[696] Among the top five causes to the disruption of supply chains in 2018 and 2019, were unplanned IT or telecommunications outages and cyber – attack and data breach. In the 2019 BCI Supply Chain

[694] ibid paras 40-44 and 53-55.
< https://casetext.com/case/columbia-casualty-co-v-cottage-health-system> accessed 25 September 2022.
[695] Tokio Marine HCC, 'Professional Risks: Cyber Security Wording 0417- General Conditions: Reasonable steps to avoid loss' (October 2017)
<https://www.tmhcc.com/-/media/RoW/Documents/PI/Cyber/Cyber-Security-Insurance-Wording-0417.pdf> accessed 25 September 2022.
[696] Enisa, 'Port Cyber: Good practices for cybersecurity in the maritime sector' (November 2019)
<https://safety4sea.com/wp-content/uploads/2019/12/Enisa-Port-cybersecurity-2019_12.pdf > accessed 25 September 2022.

Resilience Report, 44.1% of the participating organizations reported unplanned IT or telecommunications outages caused the disruptions to supply chains while 26.1% of the organisations reported supply chain disruptions were caused by cyber and data breach. While this is an alarming figure, it is an improvement to the 30.3% in 2018[697] but less than the 33.3% of the organisations in 2020 that reported disruptions caused by cyber-attacks or data breaches.[698] The COVID-19 pandemic is a contributing factor to the increases in cyber -attack disruptions to supply chains in 2021. Even though cyber-attacks and data breaches only caused just over a quarter of supply chain disruptions in 2019, the survey revealed that 61.7% and 52.9% of the respondents believed that cyber risk is the major cause of concern to the efficient and risk free functioning of supply chains in 2020 and 2022 respectively.[699]

5.81. The insurance implications of a disruption to the supply chain of the companies operating from the port and those indirectly relying on its services will be significant. The fall out along the supply chain is primarily based on the fact the Peel Ports Group which manages the Port of Liverpool is 'the second largest port group in the UK, handling over 70 million tonnes of cargo per year and 15% of the UK's total port traffic through its waters'.[700] The Port of Liverpool and its sister ports that form the Peel Group are centred in the Irish Sea with locations in Dublin, Glasgow and the Manchester Ship Canal. They have direct access to North West of England and the main RoRo services to Ireland and oil, gas and windfarm installations in the Southern North Sea.[701] Many businesses rent spaces and operate from the port facilities. A competitive advantage of the Port of Liverpool is the new in river deep water container terminal, Liverpool 2 which has the capacity to accommodate the world's largest container vessels bearing in mind as well that it

[697] Business Continuity Institute, 'Supply Chain Resilience Report 2019: Causes and Consequences of Supply Chain Disruptions' (2019) 24. <https://www.zurich.co.uk/-/media/news-and-insight/documents/useful-documents/bci_supply_chain_resilience_report_october_2019.pdf> accessed 22 September 2022.
[698] Ibid 30.
[699] Business Continuity Institute 2019 (n 697) 27; Business Continuity Institute, 'Supply Chain Resilience Report 2021' (2021) 31,34. <https://www.thebci.org/static/e02a3e5f-82e5-4ff1-b8bc61de9657e9c8/BCI-0007h-Supply-Chain-Resilience-ReportLow-Singles.pdf> accessed 22 September 2022.
[700] Peel Ports Group, 'Investor relations' (2022) < https://www.peelports.com/investor-relationss> accessed 22 September 2022.
[701] Ibid.

is estimated that 35 million consumers live within 150 miles of the Port of Liverpool.[702] The other terminal in Liverpool is the Royal Seaforth Container Terminal (RSCT) which has sea connections to the USA, Canada, Spain, Italy, Portugal, Cyprus and Turkey and feeder services connecting Liverpool with the Far East, India, Africa and South America.[703] The extensive geographical reach of the Ports of Liverpool, its container capacity and the volume of trade it facilitates explains why it is logical to expect significant aggregation losses from a cyber-attack of this nature.

5.82 The exact impact may not be known as many companies especially SME will struggle to quantify how much of the losses incurred were insured as reflected in the 45.2% of organizations that experienced significant supply chain disruptions and were unable to quantify their losses in the BCI Supply Chain Resilience Report 2019.[704] The capacity to quantify the financial losses from a supply chain disruption is important for a business to identify the most appropriate remedy and business continuity plans, be it insurance and or any other feasible option.[705] For the organizations that could quantify their financial losses, 76.2% reported full or partial coverage of financial loss in 2021[706] compared to the 56.9% in 2019 and 48.9% in 2018 that had partial insurance. As the 2019 the report pointed out, between 2018 and 2019 there was an 8% increase in the number of organizations that insured a portion of their financial losses that were due to disruptions in their supply chains, therefore organizations are doing better at identifying potential disruptions and purchasing adequate insurance coverage. On a positive note, more companies are aware of the non-physical risk to their supply chain. Between 2018 and 2019, there was a reduction from 21.9% to 14.3% of organizations indicating that 'they only have insurance for traditional physical damage, and they were not aware of non-damage supply chain cover.'[707] These figures changed to 8.2% and 9.4% respectively of the companies who reported their insurance did not

[702] Ibid.
[703] Peel Ports Group (n 700).
[704] Rachael Elliott, Catherine Thomas and Kamal Muhammad, 'Supply Chain Resilience Report 2019: Causes and Consequences of Supply Chain Disruptions' (Business Continuity Institute and Zurich Insurance, 2019) 34. <https://www.thebci.org/static/e5803f73-e3d5-4d78-9efb2f983f25a64d/BCISupplyChainResilienceReportOctober2019SingleLow1.pdf> accessed 22 September 2022.
[705] ibid.
[706] Rachael Elliott, 'Supply Chain Resilience Report 2021' (BCI and Zurich Insurance, 2021) 41 <https://www.thebci.org/static/e02a3e5f-82e5-4ff1-b8bc61de9657e9c8/BCI-0007h-Supply-Chain-Resilience-ReportLow-Singles.pdf> accessed 22 September 2022.
[707] Elliott, Thomas and Muhammad (n 704) 34.

cover the full financial impact of disruptions because their policy only covered traditional physical damage events or they were not aware of new non damage supply chain covers.[708] Inevitably, the economic fallout from a cyber-attack which affects a global supply chain is very high. The Bashe attack which is a hypothetical scenario of a malware affecting thousands of companies with a ransomware showed that such a global cyber-attack on the world economy would range between '$85 to $193 billion from the least to most severe[709] scenario variant'.[710] Business interruption losses accounted for 71% of the total loss in the least severe variant and 59% for the most severe.[711]

5.83. The risks of loss to so many customers and suppliers due to the DOS attack on the Port of Liverpool means aggregation of loss is possible. Aggregation of loss occurs where two or more losses are treated as a single loss where they are connected by a unifying factor.[712] The first well known incidence of aggregation from a cyber-attack came after NotPetya and WannaCry in 2017 which affected more than 300, 000 devices in 150 countries at the same time. Following NotPetya ransomware, A.P. Moller -Maersk which is the largest container shipping company had to 'reinstall over 4000 servers, 45 000 PC's and 2500 applications, estimated to costs up to $300 million'[713]. Merck was another company affected by NotPetya that claimed in excess of $1.3 billion in losses from their insurers mostly from business interruption losses.[714] Though Merck had

[708]Elliott (n 706) 43.

[709] A ransomware attack that encrypts data on infected devices running operating system A which compromises 43.1% of all global devices (S1). The mid-level variant (S2), the encryptor has ability to impact devices on both Operating system A and B, 97.3% of all devices worldwide. The most severe variant (X1), malware encryptor for company devices and backup wiper that can impact devices running both A and B operating systems, also 97.3% of world devices.

[710] Cambridge Centre for Risk Studies, Lloyd's of London and Nanyang Technological University, 'Bashe attack: Global infection by contagious malware' (CyRim report, 2019) < https://www.lloyds.com/cyrim> accessed 25 September 2022.

[711] Ibid.

[712] For a detailed discussion of Cyber Risks Reinsurance, Modelling and Accumulation, see Celso de Azevedo, 'Cyber Risks Insurance: Law and Practice (1st edn, Sweet & Maxwell 2019), para 11-001 – 11-029.

[713]Cambridge, Lloyd's and Nanyang 'Bashe attack' (n 710) 15.

[714] Jon Bateman, 'War, Terrorism and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions' (Carnegie Endowment For International Peace, 05 October 2020) 7 <https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819> accessed 25 September 2022; David Voreacos, Katherine Chiglinsky and Riley Griffin, 'Merck Cyberattack's $1.3 Billion Question: Was it an Act of War?' *Bloomberg Markets* (London, 3 December 2019) <https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war > accessed 25 September 2022.

cyber insurance, the limits were too low to cover all their loss, so they relied on some of their property and casualty insurance. WannaCry caused an estimated $8 billion in losses to businesses which could have easily surpassed those figures had it not been for limitations in the malware created by the hackers.[715]

b. Aggregation of Loss Express Provision

5.84. Cyber insurance policies usually incorporate sub-limits and deductibles for the different types of coverage within the policy and is one of the techniques used by insurers to manage their exposure. For example, in Tokio Marine HCC cyber security policy 0417, the cyber business interruption clause includes a maximum liability of GBP 250,000. The clause provides:

> The Insurer agrees that if during the Period of insurance the Insured suffers a reduction in Business income as a result of the actions of a Hacker or contracted Virus causing a total or partial interruption, degradation in service, or collapse of the Insured's Computer systems the Insurer will indemnify the Insured for said reduction in Business income and Increased costs of working incurred by the Insured during the Period of restoration
>
> Provided that the Insurer's maximum liability will not exceed GBP 250,000 (unless stated otherwise in the Schedule) for expenses necessarily incurred in respect of any one Claim and in total for all Claims first made during the Period of insurance.[716]

Aggregation clauses allow two or more distinct losses to be joined as a single loss when they are linked by a unifying factor.[717] Assureds rely on aggregation clauses often to meet or cap the deductible per claim so they gain the right to recovery of an indemnity from their insurer while insurers rely on aggregation clauses to limit their liability by capping the sum insured.[718] An

---

For a detailed history of the events see Andrew Coburn and others, 'Cyber risk outlook' (Centre for Risk Studies, University of Cambridge in collaboration with Risk Management Solutions Inc, 2019) 25 <http://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2019.pdf> 25 September 2022.

[715] Cambridge, Lloyd's and Nanyang 'Bashe attack' (n 710) 13.

[716] Tokio Marine HCC, 'Professional Risks: Cyber Security Wording 0417- Cyber business interruption cover' (October 2017) <https://www.tmhcc.com/-/media/RoW/Documents/PI/Cyber/Cyber-Security-Insurance-Wording-0417.pdf> accessed 22 December 2021.

[717] *Lloyds TSB General Insurance Holdings Ltd v Lloyds Bank Group Insurance Co Ltd* [2003] Lloyd's Rep IR 623; [2003] 4 All ER 43 [30] (Lord Hobhouse SCJ).

[718] *AIG Europe Ltd v OC320301 LLP (formerly the International Law Partnership LLP) and others* [2017] UKSC 18; [2018]1 All ER 936 [14] (Lord Toulson SCJ).

important exercise when discussing aggregation[719] is understanding the meaning or construction of the aggregation of loss clause present in the policy. In construing aggregation clauses, there must be a balancing exercise so that they are neither narrowly or broadly interpreted;[720] 'the safe course is to fall back on the words actually used, and to read them as they stand'[721]. There are policies that do not expressly include aggregation clauses, in that case the overall structure of the agreement will determine if the reassured is entitled to aggregate losses so that there is one (1) deductible, or the reinsurers can aggregate losses so that there is a single limit of liability. If the assured policy included the cyber business interruption clause mentioned above, the relevant question is what constitutes a claim? Will the business interruption resulting from each cyber security breach constitute a separate claim? Will the claim include third party claims against the assured? The policy defines a claim as a demand for financial compensation, notice of an intention to commence legal proceedings, or request for reimbursement following a loss against the insured. By this definition, it is correct to state that a claim will include third party liabilities against the assured for which he seeks compensation from the insurers.

5.85. Even if each cyber security breach at the Port is accepted as a separate claim and the business income and increased costs of working exceeds GBP 250,000, the insurers will not be liable as the maximum limit of GBP 250, 000 applies both for a single claim and for the aggregate of all claims first made during the period of insurance. By choosing to structure the clause this way, the insurer manages his overall exposure by limiting his liability to an agreed sum despite the number of claims by the assured or the number of claims against the assured for example from dependent businesses along the supply chain. It is also less ambiguous to categorise the limits in relation to each claim rather than an occurrence or event which is difficult to pinpoint with cyber risks and incidents. The risk to the insurers is just as dire if they have multiple assureds who have been affected by the same incident at the port and who seek indemnity from the insurer for each

[719] For a detailed discussion of cyber risks reinsurance, see chapter 11 in Celso de Azevedo, *Cyber Risks Insurance Law and Practice* (1st edn, Sweet & Maxwell 2019).

[720] *Spire Healthcare Ltd v Royal & Sun Alliance Insurance Ltd* [2022] EWCA Civ 17 [9] (Lady Justice Andrews); *Lloyds TSB General Insurance Holdings Ltd v Lloyds Bank Group Insurance Co Ltd* [2003] Lloyd's Rep IR 623; [2003] 4 All ER 43 [30] (Lord Hobhouse); *AIG Europe Ltd v Woodman* [2017] Lloyd's Rep IR 209; [2017] 1 WLR 1168 [14] (Lord Toulson JSC).

[721] *Axa Reinsurance (UK) Ltd v Field* (1996) 1 WLR 1026, 1035.

claim which is be paid at the maximum aggregate limit allowed under the policy. For the business interruption aspect of the policy alone, the insurer could be expected to pay millions, an estimate which has not yet considered the other losses and liabilities incurred due to the breach for example legal and defence costs, expert consultant fees to negotiate with the hackers regarding the ransom demand, reputation damage and all the other expenses and liabilities incurred while the Port 's functions were interrupted.

5.86. Other clauses will include reference to occurrences or event, the effect of which will also depend on the construction of the clause itself. The clause may include the following or similar words:

> Underwriters hereon shall not be liable for more than the sum insured as stated in the Schedule in respect of each occurrence… In no event shall the liability for any one occurrence under this policy exceed…
>
> Deductible- Each loss shall be adjusted separately and from the amount of each such adjusted loss a deductible of USD 100,000…
>
> Occurrence means any one loss and or series of losses commencing during the Policy Period and arising out of and directly occasioned by one Cyber Attack

There is reference to 'each occurrence, each loss' and 'an occurrence' is defined as any one loss and or series of losses commencing during the policy period…, therefore it appears that occurrence is used to indicate a loss with the emphasis on the time of loss and the requirement that it commences during the policy period, more formerly known as 'occurrence basis' or on a 'losses occurring basis'.[722] There is an agreed limit of the sum an insurer will pay for each occurrence and by definition the said limit also applies series of losses.

III. Chapter Summary

Traditional Marine Insurance Policies

- Traditional marine hull and cargo insurance policies do not cover BI and reputational damage loss that occurred at the port of Liverpool. Marine policies usually exclude liability

[722] *Wasa International Insurance Co Ltd v Lexington Insurance Co* [2009] UKHL 40; [2009] 4 All ER 909 [74] (Lord Collins).

from cyber / computer related risks used to inflict harm or from the failure, error, malfunction of any computer system or any other electronic system. Therefore, the port of Liverpool nor the shipowners using the port would be able to recover an indemnity from their traditional marine insurers.

- ICC cargo forms do not provide for or exclude loss or damage from cyber risks. Liverpool port authority and other cargo owners have several endorsements and cyber-attack exclusion and writebacks clauses that may be added to traditional cargo policies so that an assured is partially protected for physical damage or loss, but in limited circumstances such as where the assured is: i) the sole victim or target of the attack (JC2019-004, JS2018-001and JS2019-005) or ii) at the time of the loss the insured property was onboard a conveyance (JC2019-004).

- Another set of clauses (JC2020-014 and JS2019-006, if added will protect the assured from physical loss or damage where the computer systems were not used to inflict harm on the assured, in some instances subject to its attachment to policies covering war risks, terrorism or political motive and or targeted attacks.

- If attached to a war risk policy, Cyber Coverage Clause (Targeted Cyber Attack Write-Back) (JS2019-006) the assured will be covered for loss that would normally be covered where: i) the computer was used in the launch, guidance system and or firing mechanism of any tangible weapon or missile or ii) where the physical loss or damage would be normally covered if such loss was caused by a targeted attack.

- Similarly, CL437 is a writeback of CL.380 but includes non-malicious loss or damage and operates as a paramount clause except when added to the Institute War Clauses. The clause is a writeback of physical damage or loss, general average or salvage charges where directly caused by a list of named perils which results from a computer system, software programme, code or process or any other electronic system or from the failure or malfunction of any computer system.

- Even if cyber risks are not listed among the excluded perils and are ‘silent risks’ (no longer the practise), traditional insurance policies will not adequately cover the unique nonphysical loss

that resulted from the DOS attack at the ports. Adding an endorsement or cyber exclusion writeback clauses are also not comprehensive protection for an assured. These requirements along with express limits of liability for ‘each and every loss, or series of losses arising out of one event’ and ‘an annual limit of aggregation’ are methods used to reduce the risks of systemic loss and aggregation of loss.

UK Standard Business Interruption Form

- Standard BI policies cover first party risks but not loss caused directly or indirectly from a DOS attack where there was no physical damage or loss. This is mainly because the insurers are exempt from liability for consequential losses arising directly or indirectly from erasure, loss, distortion or corruption of information on computer systems, records programs or software caused deliberately by individuals within named categories including malicious persons.

- Similarly, BI policies do not cover liabilities to third parties for example partners along the supply chain whose trade was disrupted, or cargo damaged as a result of the interruption to the assured’s business from a cyber-attack. This demonstrates the inapplicability of standard UK business interruption policies to cover cyber related risks and losses. Accordingly, bespoke cyber BI clauses and policies must be created to cover the specific risks and losses that will arise where business interruption and reputational damage are the result of a cyber incident.

- The doubt regarding the meaning of ‘other property’ as referenced in the UK Standard BI form will be removed if nonphysical losses for e.g., loss or damage of data or software are overtly excluded and or the definition of ‘other property’ is explicitly stated. However, reference to ‘building or other property’ in the UK Standard BI form, suggests that loss or damage to data or software are unlikely to be covered since they not occupy a physical state or of the same genus as ‘building’.

- Cyber risks BI policies will not generally respond to claims for physical injury or destruction of tangible property including cargo that has been stolen during a cyber-attack.

- Cyber policies vary regarding the expenses that will be covered by an insurer during business interruption arising directly or indirectly from a cyber-attack. Depending on the policy, Liverpool Port authorities may not be covered for normal overhead costs, general business expenses, salaries or wages incurred by the assured during the period of interruption. There are other policies which will indemnify the assured for normal operating expenses including payroll on condition that such expenses continue during the period of restoration. Forensics expenses to investigate the source of the interruption to the business may or may not be covered by business interruption insurers.

- Legal costs and expenses are excluded from many cyber BI policies however the costs to retain an expert to negotiate ransoms with hackers are usually covered. Though the costs to retain an expert negotiator is frequently found in cyber insurance policies, the limits of protection may not be as high as those offered in Kidnap & Ransom (K&R) policies, so while some protection is given, it may be too low for the extent of damage or the high sums that may arise from a ransomware and a DOS attack on the port system. Some insurers offer cyber risks extensions to their K&R policies which means the assured will have access not only to the higher limits of protection, but the expert teams trained to negotiate and deal with ransom demands and kidnapping.

Reputation Harm

- Multiple cyber-attacks that target the Ports of Liverpool and which are widely publicized will inevitably lead to reputational damage. Most reputational harm policies provide that the insurer will only reimburse the assured for reasonable and in some instances proportionate measures taken to protect or re-establish the reputation of the business and not the reputational damage itself.

- Reputational harm insurance does not usually protect against pre-loss crisis costs, loss or crisis costs arising from a cyber incident, so the Ports authority could not rely on such policy to cover those expenses. However, reputation protection clauses are regularly found within cyber

insurance policies that will cover public relations costs, loss of income and the additional expenses resulting solely and directly from the damage to the reputation of the business.

- Security management must now include considerations about reputational damage from cyber-attacks / incidents along with the development, communication and execution of a strategy to repair the reputation of the business / company and the same applies even to an assured port authority.

Way Forward

- A good option for the assured port operator will be provided under a cyber insurance policy, a cyber business insurance policy. However, cargo loss may be excluded under standalone cyber policies so the assured must make sure that their cargo policies include a cyber extension clause.

- Hybrid policies (for example Property business interruption combined with technological) are being offered in the London insurance market to cover both physical and non-physical cyber related loss. This provides the most comprehensive insurance option for Liverpool Port authority and other assureds who may also be indemnified for cargo loss or other physical damage arising from a cyber-attack. However, the physical property would need to be covered elsewhere, for example under an unrelated cargo policy before the insurer of the blended / hybrid policy would indemnify the assured for those losses.

- Following Lloyds Bulletin Y5258, insurers must amend the UK Standard BI form to include a clause stating their position as it relates to business interruption arising from or attributable to a cyber-attack.

- Port operators must invest in the training of their staff at all levels of the workforce and ensure that third party companies are certified and constantly updating their systems, so they are as cyber secure as possible. Each stakeholder must request that partners along the supply chain are at minimum adhering to industry guidelines and perform regular updates, training and penetration testing. There needs to be a uniformed cybersecurity certification for port facilities

and cybersecurity commitments / warranties need to become a standard clause in all commercial contracts however each clause must be drafted to reflect the evolving nature of cyber risks. Small and medium sized businesses will be able to access and afford these services through the pooling of resources.

Conclusion

The scenarios discussed throughout this research highlighted the main concerns relating to the vulnerability of the marine sector to cyber risks. While cyber risks are not new, the selected method of investigation which permitted a detailed analysis of the issues in marine specific scenarios and the examination of available marine and cyber insurance policies to test the adequacy of insurance currently offered to assureds and other stakeholder in the sector against cyber risks is unchartered territory.

The following principles are the main conclusions from the research, each of which is supported by examples from points discussed in the scenarios. The final section of the concluding remarks will present the researcher's suggestions/ recommendations based on the gaps and or ambiguities identified during the research relating to cyber insurance coverage in the marine sector.

General Principle 1: Traditional marine insurance policies do not adequately protect an assured against cyber risks either because of the exclusions added to the policy or the focus on physical damage and marine perils.

A loss or damage proximately caused by or arising from a cyber incident may, in some instances be covered under traditional insurance policies. Notwithstanding, traditional marine insurance policies[723] will not adequately protect an assured against the loss or liabilities caused by or arising from cyber risks. This is partly because cyber risks are not always expressly provided for or excluded in traditional marine insurance policies. Accordingly, where a cyber-attack is deemed to be the proximate cause of the loss and there is a cyber exclusion clause, these policies either will not, or in some instances will provide limited protection to an assured against most of the unique nonphysical losses or liabilities that may result from a cyber security breach. Conversely, without a cyber exclusion clause in traditional marine insurance policies, there is the potential for multiple claims against insurers, requesting that they cover loss or damage to IT and OT technology such as GPS, ECDIS devices, damage or loss to computer software and hardware as well as nonphysical

[723] For the purposes of this research, reference to traditional marine insurance means Marine Hull & Machinery, Marine Cargo Insurance, P&I insurance and K&R policies.

financial loss including data loss, ransoms, business interruption loss and reputational harm. Damage and Loss of that nature were not the type envisioned by marine insurers at the time of contract, thus they will be exposed to unexpected and unintended liabilities. At the same time, shipowners or charterers who assumed that some degree of cyber risks protection was guaranteed under their H&M or cargo insurance will recognize that they are either uninsured or underinsured. By being uninsured or underinsured for extended periods with increasing liabilities, assureds will eventually get to a financial state where they risk being unable to repair the damage or reimburse others for the loss caused by the cyber incident, ultimately dishonouring many contractual obligations. Consequently, H&M, cargo policies, war risk policies and P&I insurance may offer some protection against cyber risks, however such coverage will be inadequate as it will be limited to conventional marine perils and excludes specific cyber risks such as software and data loss, incident response and recovery costs, regulatory fines, intellectual property theft, business, and contingent business interruption losses inter alia. H&M insurers may reject any claim initiated by an assured arising from a cyber-attack, computer or electronic risks that results in nonphysical damage onboard the vessel. Business interruption loss and reputational harm following for example the DOS attack at the port of Liverpool discussed in scenario 4 are examples of the nonphysical losses or liabilities which may result from a cyber-attack / incident. As revealed in the discussion of the issues in the scenario, the BI and reputational damage loss from that incident would not have been covered under any of the traditional marine insurance policies. A H&M insurer will respond to damage to hull and machinery of the insured vessel or property thereon or damage caused by the insured vessel to another vessel but not usually to a loss or damage in which there is no physical damage. Cargo insurance covers the risk of loss or damage to cargo from all risks excepts those excluded in ICC (A) and due to the named perils in ICC (B) and ICC (C) but in their unamended form do not exclude or affirm the risk of loss from a cyber-attack / incident. In the same way, property BI insurers would not respond to any claim against them for the damage or loss of cargo due to a cyber-attack primarily because the property described in these policies are usually buildings and even if not, must have been used for the purpose of the business and its damage or loss has caused the assured business to be interrupted. As illustrated in the discussion of the issue in scenario 4, cargo damaged or lost because of a cyber-attack is not usually the cause

of the business interruption, rather it is a consequence of the business interruption or cyber-attack and thus would not be a liability readily accepted by property business interruption insurers.

Another reason why traditional marine insurance policies are not ideal to protect against cyber risks is demonstrated in scenario 1 where there was a cyber piracy attack and uncertainties arose as to whether there would be P&I insurance coverage to the assureds for the loss from the piracy attack. There is no general exclusion of cyber risks and piracy in P&I club rules therefore third-party liabilities that are usually insured by P&I clubs will remain covered when arising from a cyber piracy incident provided weapons of war and terrorism exclusions are not triggered. As for the ransom that was demanded by the pirates, P&I insurers position is that they will not indemnify a shipowner for monies paid as ransom to pirates whether the circumstances in which the ransom demand was made included a cyber element or not. The method of payment and the form in which the sum is tendered will not alter the position of the P&I insurers. Nevertheless, P&I clubs members committee may exercise their discretion, though rarely, under their omnibus rule by deciding to indemnify an assured for the ransom paid to pirates or cyber criminals, however there is no legal obligation to do so. Prior to ***PRA SS4/17 recommendations*** and ***Lloyds Market Bulletin Y5258*** instructing insurers to state in each policy whether they will cover or exclude cyber risks and ***IMO MSC 428/98*** recommending that safety management systems address cyber risks, the omnibus rule would possibly have played a more significant role in helping to protect shipowners from cyber and other new risks which do not fall squarely within the ambit of P&I coverage but can be classified as 'liabilities, losses, costs and expenses incidental to the business of owning, operating or managing of a ship'.

In some instances, P&I clubs may reimburse shipowners for cargo contribution to which they would be entitled but which is irrecoverable due to the unseaworthiness of the vessel based on its non-existent or poor cyber risk management, so long as the breach does not also affect club cover. Alternatively, and as shown in the arguments presented in scenario 1, assureds may resort to other insurance principles as the basis on which they can make a claim to their insurers for the loss incurred from the cyber-attack / incident. Even if assureds attempt to rely on the principles of constructive total loss, sue & labour or general average contributions, there is no guarantee that

any of these arguments will be successful. A claim on the grounds of constructive total loss is expected to fail where there is a demand for a ransom by cyber pirates since permanent deprival of access to the vessel is unlikely and efforts to negotiate a ransom is not behaviour to support a claim of abandonment on the basis that actual total loss was unavoidable as per s. 60(1) of the MIA 1906. It is equally doubtful that a temporary denial of service or a complete system wipe due to a malicious code without more will lead to a successful claim for constructive total loss. The position reverses if the cyber-attack led to a collision which caused such extensive damage that it is economically unfeasible to repair the vessel or alternatively if the pirates were more interested in keeping the vessel and cargo rather than a request for a ransom.

If there is no cyber exclusion clause, an assured who experiences loss or damage from a pirate attack that is equally attributable to the efforts of cyber criminals is likely to claim successfully against their hull insurers. The ransom and the negotiation costs may qualify as sue and labour expenses consistent with s. ***78 (4) of the Marine Insurance Act 1906 (MIA)*** and ***clauses 11.1, 11.2 and 9.1, 9.2 of the ITCH and IVCH 1995,*** provided the standard clauses are unamended. This is because the shipowner's decision to pay the ransom and negotiation fees to release the vessel and crew assisted to minimize or avert loss or damage to the vessel including its I.T and OT systems and protect the welfare of the crew. Alternatively, an assured who is coerced to pay or respond to ransom demand from a cyber-attack may recover the expenses incurred as a general average contribution or sacrifice since paying the ransom may be the most reasonable and effective option available to preserve the vessel, its cargo and secure the lives of crew members.

There are insurance policies, for example the Beazley marine piracy insurance policy discussed in scenario 1 that will indemnify the assured for the ransom paid, loss of ransom while in transit as well as effective crisis management to remedy the effects from the piracy. It is unclear whether similar terms will be applied when the request is for the ransom to be paid in cryptocurrencies, however the fact that bitcoins are used for many ransomware payments is indicative of the need to have cryptocurrency payment arrangements pre-established in the cyber incident response plan and insurance policies. However, when dealing with cryptocurrencies the parties must consider

the financial crime concerns and the best practice recommendations identified in Lloyds Performance Management Supplemental Requirements & Guidance, published July 2020.

Prior to PRA and Lloyds guidelines on clarity of cyber risks in policies, P&I clubs generally did not exclude cyber risk except for some war risks P&I clubs. The general position is that a member's P&I club will continue to cover P&I liabilities arising from a cyber risk providing the cyber-attack does not amount to a terrorist or war risk excluded under the rules. Despite the absence of a cyber exclusion clause, shipowners will still be left uninsured for some cyber related loss such as the loss of hire in scenario 2, the data loss after the data breach in scenario 3 and the costs to restore systems for example after the DOS attack in scenario 4. Whereas some P&I clubs' rules have not addressed cyber risks, others under their 'Bio chem and virus' clause have excluded cover for losses, liabilities, costs or expenses directly or indirectly caused by or contributed to or arising from the use or operation as means for inflicting harm of any computer virus. This creates an insurance gap if the cyber-attack can also be classified as a war risk, resulting in the shipowner being uninsured against such P&I loss and liabilities. This situation becomes more complex with the recent publication of cyber war exclusions clauses (LMA 5464-7) designed for cyber insurance policies in compliance with Lloyds guidance which requires that war risks are excluded in all other types of insurance.

K&R insurance is popular among stakeholders within the marine sector and providing there is no cyber exclusion clause, will offer some degree of coverage to an assured who experiences a cyber piracy attack identical to scenario 1 resulting in the payment of a ransom to secure the release of the vessel and its crew. This coverage will be found under the extortion clauses of K&R insurance which were created to address piracy risks and ransom payments, so they offer services which a H&M or war risks insurer would not provide. Therefore, even if the K&R policy is silent on cyber risks, K&R insurers would cover other nonphysical losses and provide services such as ransom to release the crew and an additional layer of protection for the ship, consultation costs, insurance for the ransom while in transit, interpreter fees, independent negotiator, medical and psychiatric assessment inter alia. Even though marine K&R policies will cover many of the liabilities that arise from a cyber piracy attack, since they were not designed for the ransomware component of

the risks, their pre-agreed limits for pay out tends be lower than what a cyber policy would provide thus inherently leaving the assured underinsured as the limits allocated are unable to match the potential scale of damage from the cyber incident / attack. Insurers of K&R policies have managed their exposure to cyber extortion by including deductibles in their policy and or limit payout for cyber extortion. Furthermore, if a K&R policy includes cyber extortion coverage, some insurers will not cover costs they believe are best placed under a cyber insurance policy. Accordingly cyber forensic costs, breach response and notifications costs, the costs for retaining counsel who specializes in privacy rights and costs for data restoration and legal liability are not covered. So, while an assured will be protected against the traditional piracy and the ransom costs, [s]he will not be adequately protected against the more cyber specific loss. Other forms of nonmarine insurance policies for example the Reputational harm policies do not usually protect against pre-loss crisis costs, loss or crisis costs arising from a cyber incident. Therefore, even if the Liverpool port authorities in scenario 4 had a reputational harm policy in place at the time of the incident, it is unlikely that the assured would be indemnified by their insurers for reputational damage caused by the cyber-attacks upon the port.

Traditional marine insurance policies do not provide any protection against liabilities or losses incurred as a result of a data breach. While data breach can occur on any type of vessel or marine facility, the vulnerability and valuable database of customer information held by passenger vessels cause them to be lucrative targets for a data breach, hence the discussion in scenario 3. The conservative view is that a data breach or cyber-attack cannot be considered a shipping incident synonymous with those named in the Athens Convention. On this basis it is accepted that the strict liability regime of the Athens Convention would not apply to a data breach and the burden would be on the claimants to establish on a balance of probabilities that the shipowners' company should be held responsible for losses arising from the data breach. Moreover, the issues discussed in scenario 3 approves the principle that an employer / shipowner will not be vicariously liable for losses arising from a data breach, caused by a crew member who uses his personal device to connect to the company network and in the process inadvertently infected the computer systems if the employee / crew member's actions were not closely connected to his employment and whose capacity in which he was employed changed while carrying out the act which led to the breach.

The inadvertence of the employee / crew member is irrelevant in establishing close connection. The decisions of ***WM Morrison Supermarket plc v Various Claimants [2018] All ER (D) 89; [2020] UKSC 12 and Mr A M Mohamud (in substitution for Mr A Mohamud (deceased)) (Appellant) v WM Morrison Supermarkets plc (Respondent) [2016] UKSC 11*** discussed the principles of vicarious liability and affirmed this principle.

Insurers may deny a claim on the grounds of unseaworthiness due to the lack of or inadequate cyber management and protection onboard the insured vessel. Assureds can counter any denial of claim on this ground if they can demonstrate that they have followed the best practices as recommended by industry and government regulators and that they have done all they reasonably could to ensure the crew and other employees were adequately trained to identify attack modes and respond reasonably to a breach. The procedures used to assess the cyber resilience or ability of a business to withstand any form of computerized or digital attack cannot be static and resistant to change, otherwise the evolving nature of cyber risks would not be accounted for.

General Principle 2: Adequate cyber risks protection will not be available in Standard marine insurances policies and clauses due to the presence of computer exclusions, the need for the loss or damage to be related to tangible property and cyber risks not being identified as an offhire event.

Insurance written on standard forms will not (adequately) respond to loss or damage caused by or arising from cyber risks either because i) they include a computer exclusion clause and ii) must be related to loss or destruction of or damage to property. This is equally true for standard offhire clauses which are inapplicable to events or delays caused by a cyber-attack as they do not list cyber risks as an offhire event and or their accepted interpretation will in most instances exclude cyber risks.

Standard U.K Business Interruption policy forms, cover first party risks but generally would not respond to scenario 4 nonphysical business interruption or loss consequent thereon caused directly or indirectly by a cyber-attack. Likewise, Standard U.K. BI policies do not cover liabilities to third parties for example partners along the supply chain whose trade may have been disrupted due to

the interruption to the assured's business from a cyber-attack. Cyber related loss or damage is excluded by clauses 5.3 (a) and (b) and 10.3 of the Standard U.K. "All Risks" Policy Form (BI), the former exempts insurers from any liability due to 'consequential losses arising directly or indirectly from… erasure, loss, distortion or corruption of information on computer systems or other records programs or software caused deliberately by… malicious persons and b) other erasure loss…on computer systems … unless from a defined peril in so far as it is not otherwise excluded.' Clause 10.3 excludes consequential loss in respect of computers or data processing equipment. An assured whose business interruption insurance is written on this type of form and whose business is interrupted by a cyber-attack will not be indemnified for their loss. The operation of the form in the context of a cyber-attack was discussed in relation to the DOS attack at the port of Liverpool in scenario 4. The outcome in those circumstances was that the stolen cargo, the delays and interruption to the port operations and all other consequential losses arising directly or indirectly from the erasure loss, distortion, or corruption of information on the port computer systems or other records program or software that is caused deliberately by malicious persons will not be covered by the insurer.

Another explanation for the unsuitability of Standard U.K. "All Risks" Policy Form (BI) to respond to loss arising directly or indirectly from a cyber-attack is the reference to 'building or other property' as the subject of its insuring clause. The doubt regarding the meaning of 'other property' as referenced in the form will be removed if nonphysical losses are overtly excluded and or the definition of 'other property' is clearly stated. Rules of contractual interpretation stipulate that where there is both a specific (building) and general term (other property) that deals with a particular issue, more weight is to be placed on the specific term. Accordingly, since data and software do not occupy a physical state or have the characteristics of a 'building', loss or damage to data or software for example due to the DOS attack at the port of Liverpool as discussed in the scenario 4 are unlikely to be covered under such a policy. This demonstrates the inapplicability of standard UK business interruption policies to cover cyber risks and consequent losses. Therefore, an assured whose business interruption insurance is written on the UK Standard form without a cyber extension clause or a cyber policy, would be expected to cover their losses and liabilities

directly from the business or out of pocket even though the operations of the business have been interrupted by the cyber incident.

The Institute Hull Time and Voyage Clauses (1995)[724] are another example of standard clauses which in their original form do not include a named peril that is associated directly or indirectly with losses caused by a cyber, computer, electronic or technological element. Consequently, there is no express exclusion or endorsement of loss from a cyber, computer or electronic incident. Accordingly, if there is no cyber exclusion clause incorporated in the insurance policy, an assured who experiences loss or damage from a pirate attack that is equally attributable to the efforts of cyber criminals (scenario 1) is likely to successfully claim against their hull insurers for the loss of or damage to vessel and or expenses incurred to protect it. However, there would be no coverage for costs to repair the GPS and ECDIS and computer systems and in some instances the ransom paid and the consultant fees to negotiate with the cyber criminals. So, an assured's reliance on a standard Institute clause will not fully protect against the losses from a cyber-attack for example the cyber piracy attack in scenario 1. The actions of cyber criminals and pirates will only qualify under the malicious acts exclusion as per clause 23 and 26 of IVCH and ITCH (95) respectively if the loss, damage, liability or expense arise from the detonation of an explosive or from any weapon of war and caused by a person acting maliciously or from a political motive. The exclusion may apply where cyber criminals use their hacking skills to detonate an explosive or where they form an alliance with pirates or political activists who used weapons of war to carry out the attack. The most viable option for the shipowner would be to rely on his war risks insurer to cover these losses since P&I clubs rules exclude war risks. The problem is that many war risk policies exclude cyber risks and vice versa for cyber policies particularly with the newly published cyber war exclusion clauses (LMA 5464-7) that are to be used with cyber policies. Consequently, an assured in the marine sector will need to purchase a war extension to address those type of risks.

Like standard insurance forms, standard offhire clauses that are often included in charterparty agreements will seldomly be effective in relieving charterers of their obligation to pay hire where

[724] 1995 version chosen as it is the most often adopted by stakeholders in the marine sector. These conclusions apply just the same to previous and more modern versions of the Institute Clauses in relation to cyber risks.

a cyber event / attack causes a delay or loss of time in the prosecution of a voyage. Depending on the presence and construction of an offhire clause, a cyber-attack can cause a vessel to be 'offhire' in several circumstances if the security breaches resulted in the loss of time and has hindered or prevented the full working of the vessel and it is not in an efficient state to perform the services required. For example, the cyber security vulnerabilities in the interface between the onshore network and the vessel could jeopardize the security of the cargo tracking system which during a cyber-attack would have prevented the vessel from proceeding with the loading or unloading of cargo thus raising potential arguments that the vessel is offhire. As discussed in scenario 2, a spear phishing attack may also qualify as an offhire event even in circumstances where the vessel is not completely dysfunctional, for example where there has been a partial malfunction or reduction in service performance. Where having experienced any of these incidents, a charterer delays or fail to pay hire because of the cyber-attack, the shipowner retains the right to suspend the performance of any or all obligations under the charterparty agreement but throughout the period of suspended performance, the vessel remains on hire so long as cyber risk is not among the perils named in the offhire clause. Currently, none of the standard offhire clauses list cyber-attacks or any computer related incident as an offhire event accordingly the offhire clause would not be triggered and the charterers obligations to pay the shipowner remains even if the functionality of the vessel is affected by the cyber-attack.

The construction and interpretation of standard offhire clauses is another hindrance for their effective applicability to cyber risks. An offhire clause with the words 'efficient state of the vessel' applies a more restrictive meaning in that the event or cause of the loss must be internal to the vessel itself, thus where those words are present in the offhire clause, it is unlikely that a vessel will be offhire based on a cyber-attack caused by a malicious or negligent act of a third party. Likewise, a cyber-attack will not be classified as an offhire event based on the qualification 'deficiency and or default and or strike of officers or crew' under clause 17 line 220 of the NYPE form as 'default' does not include negligence. This is correct even if the security breach was due to the negligence or failure on the part of the management team to adhere to BIMCO and other industry guidelines encouraging assureds to identify as vulnerabilities 'shipboard computer networks which lack boundary protection measures and segmentation of networks'. A spear

phishing attack and by extension a cyber-attack will not qualify as one of the named offhire events or fall into the category of 'any other cause preventing the full working of the vessel' since it is unlikely that a spear phishing attack will be related to the physical condition or efficiency of the vessel. However, a cyber-attack may qualify under the wider 'any other cause whatsoever' as the event need not be related to the physical condition or efficiency of the vessel or crew. The uncertainties surrounding whether cyber events will fit into standard offhire clauses will be eliminated when cyber-attacks or computer breaches are added to the list of offhire events or alternatively a clause explicitly declaring cyber-attacks or computer related breaches as non - offhire events.

A claim for loss of hire under clause 1(a) of the standard Loss of Charter Hire Insurance Including War (ABS 1/10/83) and Loss of Charter Hire Insurance Excluding War (ABS 1/10/83) is closely linked to a claim in consequence of loss, damage or occurrence covered in the Institute Time Clauses-Hulls (1/10/83) and loss damage or occurrence covered in the Institute War and Strikes Clauses-Hulls (1/10/83). Therefore, a cyber-attack which resulted in loss of hire devoid of physical damage or loss would not be covered under the ABS 1/10/83 unless there is an amendment to include an endorsement clause on cyber risks. This viewpoint is supported and was revived after the Court of Appeal decision in "The Wondrous"[725] where the issue was to determine whether there is a requirement for the vessel to be physically damaged before a loss of hire insurer will be engaged in the conversation as to liabilities. The Court of Appeal decided that loss or damage to the vessel is germane to a loss of hire policy, however if parties so intend, they may give the loss of hire policy wider meaning than the hull policy so that loss of hire will be recoverable irrespective of loss or damage to the vessel.

The BIMCO Non-Payment of Hire Clause for Time Charter Parties 2006 is limited in its application to cyber risks. It does not make provision for the issues discussed in scenario 2, where hire is fraudulently diverted or where a notice is served for the hire to be paid within a specified period and the subsequent difficulty or impossibility of charterers fulfilling that obligation when either or both the charterers and the shipowners' computer systems have been hacked. Suitable

[725] [1992] 2 Lloyds Rep 566.

clauses should be added to address these scenarios where the charterers failure to pay hire is due to a cyber-attack which is no fault of his or his agents and where reasonable steps have been taken to implement measures and procedures in line with industry guidelines. It is in the best interest of all the parties that the issue is rectified, and alternative measures taken to transfer hire within a reasonable time and that the vessel remains on hire. In the same way, the performance of the vessel should not be suspended or withdrawn where there is sufficient evidence of a cyber-attack that has contributed to delay in the payment of the charterer's hire.

The BIMCO Cyber security clause 2019 is progress but falls short in that it failed to clearly describe the standard to which each party is expected to implement cybersecurity plans and systems and to maintain, respond and mitigate any possible cyber-attack. Instead, the clause merely provides that cybersecurity measures and plans should be 'appropriate'. The explanation is that appropriate is used because the level of security will vary depending on various factors such as the size of the company, the geographical location, and the nature of the business. Essentially leaving cyber criminals to prey on the weakest link in the supply chain. This approach generates uncertainty and makes it difficult to have a standardized system in line with IMO Resolutions MSC.428 (98) and one in which all parties are on equal standing when at risk of or during a cyber-attack.

General Principle 3: There are limitation to cyber liability insurance in that they will not adequately protect an assured against marine loss and damage primarily because of the extensive exclusions and lower limits of liability for certain losses compared to limits in traditional marine policies.

Cyber liability insurance (CLI) provides some degree of protection against cyber risks but does not adequately protect an assured against marine loss and damage caused by or arising from cyber risks, primarily because of the extensive list of exclusions present in CLI and the lower limits of liability compared to the limits in traditional marine insurance policies.

Generally, cyber liability insurance policies include an extensive and a diverse list of exclusions denying protection against losses and perils that are expected to be covered under such policies.

The more frequently found exclusions include but are not limited to the costs of updating or upgrading the assured vessel, the cost of repairing, recreating, gathering or assembling an electronic data or computer software or the repair or replacement of any parts or components of any computer hardware, third party liability such as lawsuits, claims or demands by an employee, officer, director or partner of the assured, the economic or market value of data, punitive or exemplary damages, fines or penalties of any nature, loss of life, personal injury or illness, physical damage inter alia. CLI application to the marine sector is restricted especially with the inclusion of the personal injury or illness and physical damage exclusions since many of the liabilities incurred within the marine sector are related to the incidence of personal injury and or physical damage from a collision, loss or damage of cargo or damage to marine structures. This creates a problem for an assured in the marine sector for example the cargo owners in scenario 4 whose property sustains physical damage because of a cyber-attack, since a typical CLI policy will not cover the physical damage and a H&M or cargo insurer is likely to exclude damage caused by or arising indirectly from a cyber-attack. Furthermore, the exclusion of third-party claims in many cyber insurance policies denies assureds of the right to be indemnified or to be subrogated by insurers in individual or class action claims against the assured by employees, officers, directors, or partners.

Cyber insurance policies that exclude fines or penalties do not sufficiently protect assureds from the liabilities associated with a data breach such as the incredibly high fines that may arise from civil proceedings in court, arbitration matters and fines under the UK GDPR supplemented by the DPA 2018. The data breach onboard Santa Maria discussed in scenario 3 gave an insight in the type and extent of loss and the potential for aggregation of losses among insurers and across policy lines arising from a single incident of data breach onboard a passenger vessel. The scale of loss will rapidly increase if the cyber-attack affected all the vessels within a fleet or all the vessels transiting a port or canal.

The situation becomes more complex as there are marine cyber insurance policies whose definition of a cyber-attack does not extend to data breach as a peril insured against mainly because marine insurers will not cover loss or liability arising from a cyber-attack which causes purely non-

physical damage. Some marine insurers are also unwilling to cover the costs for any repairs, assembling, replacement of any electronic data and the costs of repairs to any computer software or hardware. A policy with such limitations does not provide adequate protection for the assured shipowner or others within the marine sector whose passenger vessel or other marine facility experiences a data breach. Scenario 3 discussion of the data breach onboard Santa Maria described the hardships an assured would experience as notifications costs, legal costs and data breach fines can be very expensive and too much for the assured to cover without the risks of bankruptcy. This indicates the need to ensure that even if the assured purchases a cyber marine policy which covers typical marine loss which has been caused from cyber risks, it is equally important that the assured managed his other cyber risks such as data breach by purchasing a standalone cyber policy that would address his cyber exposure gaps.

As mentioned above, one of the main limitations with CLI is that it focuses predominantly on the loss of personal data of the natural individual and very often exclude costs for the value of the data loss and will not pay for trade secrets or company documents. An exclusion of this nature means that companies in the marine sector will not be compensated for company data that have been loss or damaged. This includes the value of technical and scientific data such as software codes, customer / passenger lists, marketing strategies, customer financial details such as credit cards, internal cost structure, salaries, ongoing or failed research. There are CLI with data breach clauses which provide breach response services for both suspected and actual data or security breach that the assured first discovers during the period of insurance. However, what amounts to ‘suspected breach’ is undefined in the policies and it is recommended that the parties to the policy must define or give guidelines as to what qualifies as a ‘suspected breach’, otherwise time will be lost debating or seeking to establish that there was in fact a suspected security breach.

Whereas the exclusions and limitations mentioned above hinders CLI policies from providing assureds within the marine sector with adequate / comprehensive protection against cyber risks, they are still beneficial for their specialised coverage that are not usually named as perils insured against in traditional marine insurance. Many CLI include a data privacy, confidentiality and liability clause that covers legal liability, pays compensation costs and expenses for claims relating

to the breach of confidence in respect of the private information or personal data of any individual. Provision is also made for the breach of data protection regulations regardless of the extent of the damage resulting from unauthorized destruction or disclosure or unauthorized access to personal data. The insurer must be notified of the claim during the period of insurance or within for example 30 days after the expiration of the policy. The limitation with this clause is that the designated period for notification of claim after the expiration of the policy is extremely short considering the clandestine nature of cyber risks and the prolonged periods in which cyber risks or vulnerabilities can go undetectable. Additional protection for a data breach can be found under CLI policies in clauses on i) virus, hacking, denial of service and ii) network security liability. The former (i) covers any necessary and reasonably incurred costs of reinstating data on a storage device and to locate and remove detectable virus contained on any computer equipment of the assured or any outsourced service provider. The latter (ii) provides an indemnity for the negligent transmission of a virus or failure to prevent unauthorized access to the data. This clause is beneficial to assureds who are at risks of a cyber-attack partially due to their negligence in failing to institute procedures or cyber management systems that would have prevented / minimized unauthorized access to data.

Unrelated to data breach but on the point of limitation periods, CLI normally have a brief window for the notification of a claim compared to the 2-year limitation period for personal injury claims under the Athens Convention. This exposes assureds to the risks of personal injury claims even after the time excess clause provided in CLI policies has expired. It is yet to be seen whether a personal injury or death caused by a cyber related claim would be allowed under the 1974 Athens Convention Relating to the Carriage of Passengers and their Luggage by Sea as amended by the 2002 Protocol (2002 Athens Convention). As discussed in scenario 3 - Onboard data breach, depending on the nature of the damage those type of claims may qualify under the Convention as a ‘shipping incident’ more specifically a ‘defect in the ship’ the meaning of which includes malfunction, failure or non-compliance with applicable safety regulations when used for propulsion, steering, safe navigations inter alia. Such wide definition of ‘defect in ship’ would certainly support the view that a carrier may be held liable for the death, personal injury or damage to luggage caused by a cyber-attack which affects the ECDIS, AIS and any other navigational aid or equipment used for the escape, evacuation, embarkation, and disembarkation of passengers.

Many cyber insurance policies include an extortion clause which if widely construed may cover ransom expenses from a cyber piracy or other cyber related attacks. Cyber extortion clauses will also cover reasonable and necessary crisis response consultants' cost and ransom lost or stolen in transit. However, before most CLI insurers will reimburse an assured for ransom paid, there are certain conditions which must be met. These vary across policies but include the need to exercise due diligence before agreeing to pay ransom or surrender goods and services, reasonable efforts made to ensure that the threat was genuine and surrendered under duress. Some policies state that only the assured can agree to pay the ransom while others state that only a director of the targeted company can agree to pay the ransom. Assureds are also expected to inform the legal authorities about the threat or actual ransom request or allow their insurers to do so and keep insurers abreast of all developments concerning the ransom demand and threats. Despite the commitment by cyber insurers to reimburse assureds for ransom and consultation costs, whereas in scenario 1, the cyber criminals are working in tandem with pirates and the vessel and crew are detained, many of the services and cost covered under a typical K&R policy will not be recoverable from a cyber insurer. Cyber insurers are not expected to reimburse an assured for the full salary and all employment benefits due or reasonably expected based on the past performance before the insured person was kidnapped, detained, or hijacked. Cyber insurers are unlikely to cover temporary employee replacement, job retraining, personal financial loss, forensics fees, medical services, cost of childcare and cosmetic surgery, if necessary, repatriation fees and travel costs for the insured family or additional bunker costs if the pirate deviates from the intended route or steals the bunker. Moreover, if any of these claims were allowed by the cyber insurer, the limits for payout would be lower than the payout under a K&R policy.

Some policies, for example Hiscox CyberClear exclude normal overhead costs, general business expenses, salaries or wages incurred by the assured or any other person or entity. Other policies, for example Beazley Breach Response[726] will indemnify the assured for normal operating expenses including payroll on condition that such expenses continue during the period of restoration. Forensics expenses, that is the reasonable and necessary costs incurred by the assured

[726] Both the Hiscox CyberClear and Beazley Breach Response policies have been discussed in scenario 4 on Business Interruption and Reputational Damage.

to investigate the source of the interruption to the business may or may not be covered by business interruption insurers. While legal costs and expenses are excluded from many BI policies, the same cannot be said for the costs to retain an expert to negotiate ransoms with hackers. Cyber risks BI policies / clauses will not generally respond to claims for physical injury or destruction of tangible property including cargo that has been stolen during a cyber-attack. Similarly, pure cyber policies will not offer protection for cargo that is damaged or destroyed directly or indirectly from a cyber-attack, ultimately leaving an assured in marine sector without adequate protection against physical damage or loss.

Generally, CLI insurance provides a more comprehensive protection for liabilities related to a data breach than the coverage provided under a policy written specifically for hull and machinery insurance or any traditional marine policy with a cyber endorsement but for physical loss, personal injury, indemnification for third party claims and the loss of company data and trade secrets, CLI does not adequately protect an assured in the marine sector. Even cyber policies designed specifically for the marine sector excludes nonphysical loss that are commonly associated with cyber breach.

General Principle 4: Standard Cyber Exclusion clauses – relieves insurers of most but not all cyber related risks, therefore they do not operate as an absolute exclusion.

Standard cyber exclusion clauses when attached to traditional marine insurance policies will exclude most risks caused by or arising from malicious and non-malicious cyber-attacks, thereby relieving marine insurers of liability for many of the direct and consequential losses. However, with gaps identified in the construction of these cyber exclusion clauses, insurers will sometimes be found liable to indemnify assureds for losses they believe were excluded.

The discussions throughout this research identifies CL.380 and the more recently published LMA5402: Marine Cyber Exclusion clauses as one of the main reasons traditional marine and standard policies do not provide adequate insurance to assureds regarding loss or liabilities caused by or arising from cyber risks. CL.380 excludes loss from malicious cyber-attacks and is attached to most H&M and cargo insurance policies stating that “in no case shall this insurance cover loss

damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system." The correct interpretation of CL.380 in terms of whose intent to inflict harm must be established, has not been decided by a court, tribunal or any practice direction, therefore the issue remains unsettled. An insurer whose policy includes CL.380 will not eliminate the risks of liability for loss or damage caused by cyber risks in absolute, but the exclusion will only be effective against computer or electronic related risks that was 'used or operated as a means to inflict harm', thereby leaving the insurer exposed to liability for damage or loss caused by or arising from non-malicious and or accidental computer or electronic risks which was not 'used or operated as means to inflict harm'. The limitation of CL.380 was demonstrated in scenario 4 when a crew member onboard the vessel by using his USB device accidentally infected the ship internet network resulting in a data breach and loss of personal and company data. The reliance on this exclusion clause in a H&M policy or any other marine policy will not operate as an absolute exclusion since the requirement 'to inflict harm' will be difficult to establish considering that the malicious code was accidentally introduced to the vessel's internet network. Therefore, CL30 is not effective in scenarios where there was no intent to use a computer, computer system programme, malicious code, computer virus or process or any electronic system to inflict harm.

LMA5402 does not include the words 'as a means of inflicting harm' as an overriding requirement. Instead, the drafter divided the original clause 1.1 of CL.380 into two parts to create clause 1.1 and 1.2 of the LMA5402. This means that the exclusion clause becomes operative and is paramount in one of two situations first either where there is a failure, error or malfunction of any computer, computer system, computer software program, code (which is new as it did not form part of the original CL.380 clause) OR the second situation is the use or operation, as a means for inflicting harm of any computer, computer system, computer software program, malicious code, computer virus or process or any electronic system. Clause 1.1 of LMA5402 removes the deficiency of CL.380 by clarifying that non-malicious events which causes loss, such as the failure, error or malfunction of any computer system, software program or code will be excluded from coverage by insurers. Thus, if a cyber-attack is the proximate cause of the loss and cyber risks is a named

peril in the policy which also includes a LMA5402 clause, the insurer will not be liable to indemnify the assured for his loss as the exclusion clause takes precedence over the cyber risks perils clause. In other words, with incorporation of LMA5402, breaches inadvertently caused by error or omission for example the accidental and unintentional introduction of a malicious code which led to the data breach in scenario 3, would operate to relieve the insurer of any cyber related liabilities under the policy. LMA5402 has scope for wider interpretation and application than CL.380.

General Principle 5: A hybrid approach to insurance protection against cyber risks in the marine sector provides better protection to assureds.

A hybrid approach to insurance, that is a combined policy of cyber and marine perils will provide the most comprehensive protection against cyber risks to the marine sector. This combined policy may appear in different forms depending on the needs and resources of the assured namely: i) a cyber endorsement to traditional marine insurance policies or ii) separate cyber liability insurance along with their traditional marine insurance policies or the most ideal iii) a policy tailored to respond to the cyber risks prone to the marine sector and which results in traditional marine perils.

For some assureds, particularly small and medium enterprises (SME), the most affordable solution to close the gaps in their cyber insurance coverage is to purchase or make a request for a cyber endorsement to their traditional marine insurance policies. Recent endorsement clauses include LMA5403 which incorporates the original language of CL.380 in clause 1 and 3 but in clause 2 the assured will be indemnified for computer related losses ‘provided they were not used or operated as a means for inflicting harm’. While this may be a quick fix, it is not a comprehensive or adequate protection. The importance of paying attention to the language used in the endorsement clause is demonstrated in scenario 3. The data breach in that scenario was caused by the accidental introduction of a malicious code to the computer network of the shipping company. Although LMA5403 is endorsed on the assureds H&M policy, the assured may be left without coverage as it is possible that insurers may deny the claim on the basis that they do not cover damage or loss caused by the use or operation of a malicious code or virus. This is because of their omission of ‘malicious code or virus’ among the list of ‘computer systems, software programs or process or

any other electronic system' that causes loss for which the insurers agreed to indemnify the assured. Even if the malicious code or virus could fit into the causative list, the assured's claim for the loss due to the data breach would still be denied since the code / virus was used or operated as a means for inflicting harm when it led to data breach. Furthermore, most endorsement clauses will only indemnify the assured for losses recoverable under the parent policy that is caused by cyber risks. As such when written on a traditional marine policy, while the insurers may cover the cyber piracy attack in scenario 1, the assured who experienced the data loss in scenario 3 may be without cover as these are not the type of losses recoverable under a H&M policy or any other marine insurance policy. The endorsement clause is usually a write back of CL.380 cyber exclusion but the disadvantage with endorsements is that many cyber specific liabilities such as data breach and pre and post crisis management services are omitted. Furthermore, the cyber vulnerabilities of the assured would not have been assessed or provided for under the policy. So, even with a cyber endorsement, there will still be gaps in the coverage as risk unique to cyber or the appropriate limits may not have been considered.

An assured will have the most adequate protection against cyber piracy when he acquires cyber protection either through a cyber endorsement clause for example LMA5403 (Marine Cyber Endorsement) and LMA5400 (Property Cyber and Data Endorsement) incorporated within their traditional marine H&M or K&R policy or through a bespoke cyber marine insurance policy. Currently in the marine insurance market, some standalone policies are divided into operational technology protection (OTP) that covers financial loss as a result of physical damage and loss of hire arising from a cyber-attack while data and information technology protection (ITP) focuses on software and data breach. This means to get the most comprehensive coverage; the assured may need to combine for example a hull policy with an ITP or purchase both an OTP and ITP policy. Even with the combination of a hull and the OTP policies, there is no guarantee that liabilities such as ransoms, ransom in transit and the crisis management services will be covered if a loss arises from a cyber pirate attack as discussed in scenario 1 since not all insurers are prepared to cover these costs. An option would be for the assured to have OTP and ITP as a comprehensive insurance package where he would receive the crisis management services and then purchase the marine

piracy policy. This combination of policies would offer the most adequate protection against the liabilities and expenses incurred due to the cyber-attack and a traditional pirate attack.

The point was made above that ICC cargo forms do not expressly provide for or exclude loss or damage arising directly or indirectly from cyber risks, thus an assured will not be adequately protected against liabilities from cyber risks if the policy incorporates an unamended ICC A policy. Cyber endorsement clauses may be attached to these policies, but they will not provide comprehensive protection against cyber risks since the commercial impact of the endorsement clauses is limited by the restrictive language used to define its scope. Some endorsement clauses will cover physical damage and loss where the assured is sole victim or target of the cyber-attack. JC2019-004 does not apply to systemic loss, so that the assured or his property must be sole victim of the cyber-attack unless the physical damage or loss occurred while the insured property was onboard some form of conveyance. The insurers concern about aggregation risks is reflected in restricting indemnifiable systemic loss only where it occurs onboard a conveyance and express limits of liability for 'each and every loss, or series of losses arising out of one event' and 'an annual limit of aggregation'. Likewise, Cyber Attack Exclusion Clause and Write-Back (JS2018-001) and Cyber Exclusion (Targeted Cyber Attack Write-Back) (JS2019-005) covers physical loss or damage if the insured was able to establish it was the result of a targeted attack, that is the computer systems, software programme, malicious code, computer virus or process or any electronic system was used to inflict harm solely on the insured or upon the insured property. The cargo theft in scenario 4 illustrates the restrictiveness of JC2019-004, JS2018-001 and JS2019-005 as the assureds would not be compensated for loss to their cargo because they were not the sole victims of the cyber-attack and the exception to systemic loss did not apply as the cargo was not onboard any form of conveyance at the time the loss occurred.

Another set of clauses will only operate where the computer systems were not used to inflict harm on the assured, in some instances subject to its attachment to a war risks policy and or targeted attacks. With Cyber exclusion and writeback (JC2020-014), the insurer will accept liability for cyber risks if the computer … or electronic systems were not used to inflict harm except where the clause is endorsed on policies covering war risks, terrorism or political motive. Limited Cyber

Coverage Clause (Targeted Cyber Attack Write-Back) (JS2019-006) provides cover for loss or physical damage to property if the use or operation of the computer system or programme inter alia was not to inflict harm, except when the clause is attached to a war risk policy and loss would normally be covered where the computer was used in the launch and or guidance system and or firing mechanism of any tangible weapon or missile or where the physical loss or damage would be normally covered if such loss was caused by a targeted attack.

JC2020-014 (Marine Cargo Cyber Exclusion and Affirmation Endorsement) Paragraph 1 is a repeat of paragraph 1 of CL.380 effectively excluding loss, damage, liability or expense indirectly or directly caused by or contributed to by or arising from the use or operation as a means of inflicting harm any computer system, software program, malicious code, virus, computer process or any other electronic system. Paragraph 3 provides that if JC2020-014 is endorsed- on policies covering war risks, terrorism, or political motive the exclusion would not apply to losses that would otherwise be covered arising from the use of computers, computer system etc. Yet in paragraph 2, there is an affirmation of cover for loss from the use or operation of any computer, computer system, software, programme, computer process or other electronic system If such use or operation is not used or operated as a means for inflicting harm. Similarly, CL437 is a writeback of CL.380 but includes non-malicious loss or damage and operates as a paramount clause except when added to the Institute War Clauses. The clause is a writeback of physical damage or loss, general average or salvage charges where directly caused by a list of named perils which results from a computer system, software programme, code or process or any other electronic system or from the failure or malfunction of any computer system.

The problem for assureds with having any of these clauses endorsed on their cargo or hull policy is the burden to establish that they were the sole targets of the cyber-attack and deciding the impact of the clauses' focus on physical loss, damage or liability. These requirements restrict the effectiveness of the clause in protecting the assured against cyber risks especially because it is very rare that a cyber-attack will only impact the target (s) of the attack. Moreover, it is difficult for assureds to ascertain the true targets of a cyber-attack as it may be an expensive and arduous task especially for SME. Equally uncertain is whether damage or loss to dependent third parties would

prevent the assured from discharging his burden of establishing that he was the sole target of the cyber-attack, despite the evidence to support his claim. Additionally with the focus on physical loss, damage, liability or expense of the insured's property, it is uncertain whether liability and expenses must be related to the physical state of the property or if it is wide enough to include delay and other nonphysical expenses and liabilities.

General Principle 6: There is a lack of standardization in cyber insurance wordings and definitions which makes it difficult for assureds to understand the extent and scope of their cover and raises doubts about the recovery of an indemnity following loss or damage from a cyber incident / attack.

There is no accepted standard or recognized practice in the Lloyds London market regarding the perils, liabilities and expenses that will be covered in a cyber insurance policy and there is no uniformity in the meaning assigned to key terms often found in cyber insurance.

The lack of standardization in cyber insurance wording as it relates to the perils covered and excluded and the variations in the meaning assigned to key terms makes it difficult for assureds to understand the extent and scope of the insurance they are purchasing as against the options available in the market. The inconsistencies and lack of clarification in the definition of key terms used in traditional insurance policies and standard clauses is also one of the main reasons for doubts concerning recovery of an indemnity and risks of silent cyber insurance/ non-affirmative cyber risk exposures, an issue which is being addressed due to the recent guidelines from the IMO, PRA and Lloyds.

An example of the problems that may arise from the language used can be seen in scenario 1 where the meaning of 'other property' in UK Standard BI form was discussed in relation to whether it included loss or damage of data or software caused by or arising from a cyber-attack. The uncertainty regarding the meaning of 'other property' as referenced in the UK Standard BI form will be removed if nonphysical losses are overtly excluded and or the definition of 'other property' is stated. Either approach will provide an answer to the question as to whether 'other property' will include loss or damage of data or software for example due to the DOS attack at the port of Liverpool as discussed in the scenario 4 on business interruption and reputational harm. However,

based on the description of ‘building or other property’ in the UK Standard BI form, since data and software do not occupy a physical state or bear similar characteristics of a ‘building’, loss or damage to data or software are unlikely to be covered under such a policy.

Determining what qualifies as critical IT services is important to encourage the development of Parametric insurance for business interruption policies designed for small and medium sized businesses. The principle behind this type of policy is that instead of operating based on a loss occurring, that is the indemnity principle, the insurer will automatically pay if the critical IT services of the assured has been disrupted. The problem is deciding what will be critical IT services for businesses in the marine sector, thus it is necessary for guidelines or each insurance policy to define and list examples of critical services. While the list may not be exhaustive, examples will narrow and give an insight of the type of services that will be categorized as critical. Additionally, the length of time or degree to which services are to be affected to qualify as a disruption are uncertain so these must be agreed and defined in the insurance policy. Since the policy is designed to facilitate automatic payment, this will also reduce the time and expense of the claims process.

There is no formal statement from the ICO or other legal entity within the UK on whether fines and penalties imposed under the UK DPA 2018 and GDPR 2018 are insurable. This is in stark contrast to the position held by the Financial Conduct Authority, where there is explicit prohibition of the insurance of fines it has imposed for any breach of the financial regulations. So, while many insurance policies include coverage for fines and legal fees, some with the qualification, to the extent they are insurable by law, uncertainty remains in the marine sector as to whether this will include fines and penalties from the ICO.

The violation of cyber security safety regulations should not be declared ‘illegal’ as they are not of such moral turpitude to deny a ship owner or any other assured his right to insurance. The breach of marine and cyber risks safety regulations should be an issue relating to seaworthiness rather than an issue of illegality. Knowledge of the assured as to the cyber vulnerabilities of his vessel to determine seaworthiness / cyber worthiness will include the knowledge of IT and OT personnel as well as knowledge based on the best practices published and recommended by specialist organisations in the sector, for example BIMCO Guidelines on Cyber Security Onboard Ships.

The limits of liability associated with data breaches are complicated and vary across policies. There are policies that separate the aggregate limit of liability from the limit assigned to breach response services. Assessing reasonable limits for a data breach is difficult but separating this from the aggregate limit protects the interest of the assured since breach response services could quickly exhaust the aggregate limit and leave the assured without protection for other types of losses. Similar practice has been introduced for notification and credit monitoring services to data subjects. The focus is not so much the costs for notification but the number of individuals to whom notification will be provided. Once the threshold has been exceeded, the insurer has no contractual obligation to indemnify the assured for notification cost to anyone above the limit.

Large organisations including ports may seek to rely on their contingency risk policies to close gaps in their insurance coverage which traditional policies may not protect against.

Recommendations

Insurance Sector

1. Following the Lloyds Bulletin Y5258, insurers must amend the UK Standard BI form to include a clause unequivocally stating their position as it relates to business interruption arising from or attributable to a cyber-attack. The gaps in cyber insurance coverage for this type of loss means bespoke cyber-BI clauses and policies must be created to cover the specific risks and losses that will arise where business interruption and reputational damage are the result of a cyber incident. Furthermore, prudent business owners with an interest in purchasing cyber insurance must verify the extent of available coverage for overhead and business expenses that the assured may continue to incur during the period of interruption to the business.

2. A cyber-attack can cause assureds to lose substantial amounts in assets within a short time. As such, the time excess clause as it relates to business interruption must be worded to balance both the interest of the assured and that of the insurer. A clause that is reasonable and realistic which considers the possible prolonged effects of a cyber-attack, and which reduces or eliminates the time excess period is best suited to protect the interests of insurers

and assureds. A workable clause for this purpose which is in circulation among insurers and can be found in Hiscox CyberClear policy, provides: 'the indemnity period begins at the date the interruption to the business commences and lasting for the period during which the income is affected but for no longer than the number of months in the policy'. Even with the proposed wording, there is always the possibility that the financial impact from a cyber business interruption will outlast the period for which the insurer has agreed to indemnify the assured.

3. In the absence of a statement from the ICO, the London market or more specifically the marine sector must declare a unified stance on the insurability of fines, so assureds are certain about what they are purchasing when buying insurance against cyber risks and data breach. It may be worth having a two (2) limb approach by allowing insurance of fines that were not the result of gross negligence, criminal or malicious acts of the assured or his agents while fines caused by other means are uninsurable.

4. To remove the uncertainties and the questions about whether specific cyber event fits into the offhire hire clause, it is prudent to add cyber-attacks or computer related breaches to the list of offhire events.

5. In light of **PRA SS4/17**, it is good practice for insurers to state whether physical loss / damage include loss or damage to computer hardware, software, data and electronic damage. The consensus among stakeholders in the shipping industry is that intangible losses / nonphysical losses should be covered by markets with the expertise in that area, that is cyber and product liability insurers.

Market Participants

6. I recommend that assureds including port authorities implement a cyber risk aftercare plan that will continue to service financial disruptions to the business that persists after the insurance ends. The question of who bears the ongoing expenses after the restoration period expires remains unanswered, yet this must be an area of concern for any assured particularly port operators and others who are reliant both on a physical and digital supply

chain. Alternatively, assureds must negotiate for the inclusion of a period of extended coverage clause within their cyber insurance policies so the assured will continue to be indemnified by the insurer in those instances where the profit takes too long to return to the levels it was before there was an interruption to the business by the cyber-attack. Where it is not possible to negotiate for the inclusion of a period of extended coverage clause, assureds must ensure that their expected period of interruption matches the maximum period of loss provided by their cyber policy.

7. Port operators must invest in the training of their staff at all levels of the workforce and ensure that third party companies are certified and constantly updating their systems, so they are as cyber secure as possible. Monitoring along the supply chain will be difficult but each stakeholder must request that partners along the chain are at minimum adhering to industry guidelines and have regular updates, training, and penetration testing. There needs to be a uniformed cybersecurity certification for port facilities and services like UK cyber essential certification in addition to end to end encryption and double layer security passwords when suppliers are given remote access to port network and systems. Security management must now include considerations about reputational damage from cyber risk along with the development, communication, and execution of a strategy to repair the reputation of the business / company and the same applies even to an assured port authority. Furthermore, cybersecurity commitments / warranties need to become a standard clause in all commercial contracts however each clause must be drafted to reflect the evolving nature of cyber risks. Small and medium sized businesses will be able to access and afford these services through the pooling of resources within and across sectors and government and private entities.

8. To prevent a legal debate on the issue of vicarious liability, shipowners must impose security measures to prevent crew members access to the parent network and from connecting their own devices directly to the vessel. To protect the ship and offshore networks, the best practice is to segregate crew and entertainment networks from the other

ship networks and ensure proper procedures are in place for the safe use of removeable media by ensuring that all devices are scanned and encrypted.

Policy / Legal Draftsmen (Legislators)

9. The requirement of force for an incident to qualify as piracy in maritime law may need to be amended to reflect the evolving digital landscape as there will be incidents where pirates take control of vessels with little or no 'threat or use of force' in the traditional sense of the word. Accordingly, the hacking and control of the GPS and ECDIS or any secured network which leads to pirates detaining a vessel, cargo and crew against its will should satisfy the requirement of 'force' as discussed in the scenario 1 on cyber piracy. In the absence of this basic component, where a cyber element is involved, assureds will find it difficult to claim under the piracy clause within their hull or war insurance.

10. To improve the effectiveness of the Cybersecurity Clause 2019, it is recommended that there be a requirement for the maintenance of a uniformed minimum standard and not a system modelled on appropriateness as described in the explanatory notes to the clause. Such amendment will significantly reduce the impact and success of targeted attacks on businesses along the supply chain. The pooling of resources may be a viable option so that small and medium sized businesses will have access to the highest professional and technical support to implement, maintain and monitor their cyber security needs.

Bibliography

Books

Aikens R and others, Bills of Lading (3rd ed, Informa 2020)

Bennett H, *The Law of Marine Insurance* (2nd edn Oxford 2006)

Coghlin T and others, *Time Charters* (7th edn, Informa 2014)

Cyber Operations and the jus ad bellum' in Marco Roscini , *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014)

de Azevedo C, *Cyber Risks Insurance* (1st edn, Sweet & Maxwell 2019)

Direnzo J and others (eds), *Issues in Maritime Cyber Security* (Westphalia Press 2017)

Foxton D and others, *Scrutton on Charterparties & Bills of Lading* (24th edn, Sweet & Maxwell 2019)

Hazelwood S J and Semark D, *P&I Clubs Law and Practice* (4th edn, Informa 2010)

Leloudas G, 'Cyber Risk, Autonomous Operations and Risk Perceptions: Is a New Liability Paradigm Required?' in Baris Soyer and Andrew Tettenborn (editors) *Artificial Intelligence and Autonomous Shipping: Developing the International Legal Framework* (Hart Publishing 2021)

Merkin R, 'Marine Insurance Legislation' (Johanna Hjalmarsson, Aysegul Bugra and Jennifer Lavelle (eds), (5th edn, 2013)

Rose F D, 'Failure to Sue and Labour' Journal of Business Law 1990

Schmitt M N, 'The Use of Force' in Tallin *Manual 2.0 on the International Law Applicable to Cyber* Operations (2nd edition Cambridge University Press 2017)

Scrutton on Charterparties and Bills of Lading (24th edn)

Soyer B and Tettenborn A (eds) *Charterparties: law, practice and emerging legal issues* (2018, Informa)

Soyer B, *Marine Insurance Fraud* (Informa Law 2014)

---------- *Warranties in Marine Insurance* (3rd edn, Informa Law 2017)

Sozer B, 'Seaworthiness: In the Context of Cyber-risks or "Cyberworthiness" in Baris Soyer and Andrew Tettenborn (editors), *Ship Operations: New Risks, Liabilities and Technologies in the Maritime Sector* (2021, Routledge)

Todd P, Fraud & Piracy (2nd edn, Informa 2010)

Wan I, 'Causa Proxima Non Remota Spectatur: The Doctrine of Causation in the Law of Marine Insurance' (July 2003) 34 J. Mar. L. & Com.

Williams R, *Gard Guidance on Maritime Claims and Insurance* (Gard AS, 2013)

Articles and Other sources

Aon and DLA Piper, 'The price of data security- A guide to the insurability of GDPR fines across Europe' (3rd edn May 2020) <https://www.aon.com/unitedkingdom/insights/a-guide-to-the-insurability-of-gdpr-fine.jsp> accessed 24 September 2024

Aviva Insurance Ltd, 'Cyber Insurance Policy' (BCOAG15081 12.2020) <https://www.aviva.co.uk/adviser/documents/view/bcoag15081.pdf> accessed 18 September 2022

Barlyn S and Cohn C, 'Firms Turn to Kidnap Insurance Policies to Cover Ransomware Losses' (Insurance Journal, 19 May 2017) < https://www.insurancejournal.com/news/international/2017/05/19/451637.htm> accessed 25 September 2022

Beazley, 'BBR Boost Coverage Animation' (n.d) <https://player.vimeo.com/video/265762112> accessed 24 September 2022

Beazley, 'Beazley Breach Response' (nd) < https://policies.dppl.com/policy.php?policy_number=BBR-5A8ED7A3-8OEF> accessed 24 September 2022

Beazley, 'Beazley Breach Response (BBR) in Cyber & Tech: Understanding the coverage' (n.d) <https://www.beazley.com/usa/cyber_and_executive_risk/cyber_and_tech/beazley_breach_response/understanding_the_coverage.html> accessed 24 September 2022

Beazley, 'Cyber Defence for Marine' (2019) <https://www.beazley.com/documents/Factsheets/beazley-cyber-marine-brochure.pdf> accessed 18 September 2022

Beazley Insurer, 'Marine Piracy' (nd) < https://www.beazley.com/london_market/marine/marine_piracy.html> accessed 18 September 2022

Britannia P&I, 'Additional Insurances Policy Year 2022 /23' (Version 3.00, February 2022) < https://britanniapandi.com/wp-content/uploads/2022/02/Additional-Insurances-2022.pdf> accessed 18 September 2022

Bitcoin, 'Protect your privacy' (2022) < https://bitcoin.org/en/protect-your-privacy> accessed 18 September 2022

Bourne H and Schaloske H, 'Insurability of fines and penalties for breaches of the GDPR: A UK and German Perspective' (30 January 2019) < https://www.clydeco.com/blog/insurance-hub/article/insurability-of-fines-and-penalties-for-breaches-of-the-gdpr-a-uk-and-germa> accessed 24 December 2021. Now accessible at <https://www.commercialriskonline.com/wp-content/uploads/2019/02/Insurability-of-fines-and-penalties-for-GDPR.pdf> accessed 24 September 2022.

Boyes H and Isbell R, 'Code of Practice: Cyber Security for Ships' (IET 2017) <https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-for-ships/> accessed 18 September 2022

Boyes H, 'Cybersecurity and Cyber-Resilient Supply Chains' (Technology Innovation Management Review 5(4) 2015) <http://doi.org/10.22215/timreview/888> accessed 18 September 2022

BIMCO and others, 'BMP5 Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea: High Resolution' (Version 5, Witherby Publishing June 2018) <https://www.maritimeglobalsecurity.org/media/1038/bmp5-high_res.pdf > accessed 18 September 2022

BIMCO and others, 'The Guidelines on Cyber Security Onboard Ships: Version 4' (Annex 4, 2020) <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships> accessed 18 September 2022

BIMCO, ASBA and SMF, 'NYPE 2015' (2015) <https://www.bimco.org/Contracts-and-clauses/BIMCO-Contracts/~/link.aspx?_id=EEBE70C0DDB44328BFE184C79D2BA623&_z=z#> accessed 18 September 2022

BIMCO, 'ISPS /MTSA for Time Charter Parties 2005' (Originally published in BIMCO Special Circular No. 5, 15 June 2005 - BIMCO ISPS Clauses Revised) <https://www.bimco.org/contracts-and-clauses/bimco-clauses/current/isps-mtsa_clause_for_time_charter_parties_2005> accessed 18 September 2022

Burrow R K, Increased Bank Liability for Online Fraud: The Effect of Patco Construction Co. v. People's United Bank, 17 N.C. Banking Inst. 381 (2013) <https://scholarship.law.unc.edu/ncbi/vol17/iss1/16/> accessed 18 September 2022

Cravero A and Dalton P, 'Digital Assets Theft: cybersecurity' C.T.L.R. 2016, 22 (3)

CyberEdge, '2021 Cyberthreat Defense Report' (2021) <https://www.imperva.com/resources/resource-library/reports/2021-cyberthreat-defense-report-report-ty?lang=EN&asset_id=4568> accessed 18 September 2022

DLA Piper and Aon, 'The price of data security: the insurability of GDPR fines across Europe' (3rd edn, May 2020) <https://www.dlapiper.com/en/uk/insights/publications/2020/05/third-edition-of-guide-on-the-insurability-of-gdpr-fines-across-europe/> accessed 24 September 2022.

Financial Conduct Authority, 'GEN.1 Payment of Financial Penalty' (Updated 14/04/22). < https://www.handbook.fca.org.uk/handbook/GEN/6/?view=chapter > accessed 24 September 2022.

Financial Conduct Authority, 'INSPRU 1.5.33: Payment of Financial Penalties' <https://www.handbook.fca.org.uk/handbook/INSPRU/1/?view=chapter> accessed 24 September 2022.

Futurenautics, 'Crew Connectivity 2018 Survey Report' (2018) <https://www.futurenautics.com/product/2018-crew-connectivity-survey-report/> accessed 18 September 2022

Gard, 'P&I Club Rules 2022' <https://www.gard.no/web/publications/document/chapter?p_subdoc_id=1070567&p_document_id=781871> accessed 24 September 2022

Gard Rules 2022 <https://www.gard.no/web/publications/document/chapter?p_subdoc_id=1194646&p_document_id=781871> accessed 18 September 2022

GPS.gov, 'Other Global Navigation Satellite System' (last modified 19 October 2021) <https://www.gps.gov/systems/gnss/> accessed 18 September 2022

Handbook on Loss of Hire Insurance: Norwegian Hull Club <https://www.norclub.com/handbook-on-loss-of-hire-insurance/> accessed 18 September 2022

Hellenic War Risks, 'Rules 2021 and ByeLaws' <https://www.hellenicwarrisks.com/fileadmin/uploads/hellenic/Docs/PDFs/HWRB_Rulebook_2021_Policy_Year.pdf> accessed 18 September, 2022

Hiscox Cyber Clear Policy,'Cyber and data insurance' (WD-PIP-UK-CCLEAR(1) 19029 12/18) <https://www.hiscox.co.uk/sites/uk/files/documents/2019-03/19029-CyberClear-policy-wording.pdf> accessed 18 September 2022

IACS, ‘Recommendation no. 166 on Cyber Resilience’ (April 2020) (Corr.1. July 2020) < https://iacs.org.uk/publications/recommendations/161-180/rec-166-new-corr1/> accessed 18 September 2022

IBM Security, ‘Cost of a Data Breach Report 2021’ (IBM Security and Ponemon Institute, July 2021) < https://www.ibm.com/downloads/cas/OJDVQGRY> accessed 24 September 2022

ICO, ‘Information Commissioner’s Annual Report and Financial Statements 2018 -2019’ (08 July 2019) <https://ico.org.uk/media/about-the-ico/documents/4017979/annual-report-201819.pdf> accessed 24 September 2022.

ICO, ‘Penalty Notice Section 155 Data Protection Act 2018: Case ref COM0783542 British Airways plc’ (16 October 2020) <https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf> accessed 24 September 2022.

ICO, ‘Penalty Notice Section 155, Data Protection Act 2018: Case ref COM0804337 Marriott International Inc’ (30 October 2020) < https://ico.org.uk/action-weve-taken/enforcement/marriott-international-inc/> accessed 24 September 2022.

IG P&I, ‘Revised Piracy – FAQs: Revised December 2019 <https://www.igpandi.org/article/piracy-faqs-revised-december-2019> accessed 18 September 2022

IMO, ‘Guidelines on Maritime Cyber Risk Management’ (MSC-FAL.1/Cir.3, 5 July 2017) <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf> accessed 18 September 2022

IMO, ‘Guidelines on Maritime Cyber Risks Management in Safety Risks Management Systems’ (Resolution MSC.428 (98) adopted 16 June 2017) <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf> accessed 18 September 2022

IMO, ‘Maritime cyber risk’ (2019) < https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx> accessed 18 September 2022

IMO, ‘Piracy and Armed Robbery Against Ships: Guidance to shipowners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships’ (MSC.1/Circ.1334 23 June 2009) <https://www.maritimeglobalsecurity.org/media/1008/c-users-jpl-onedrive-bimco-desktop-msc1-circ1334.pdf > accessed 18 September 2022

IMO, 'Revised Interim Guidance to Shipowners, Ship Operators and Shipmasters on the Use of Privately Contracted Armed Security Personnel on Board Ships in the High Risk Area' (MSC.1/Circ.1405/Rev.2 25 May 2012) <https://www.maritimeglobalsecurity.org/media/1009/c-users-jpl-onedrive-bimco-desktop-msc1-circ1405-rev2.pdf > accessed 18 September 2022

International Organization for Standardization < https://www.iso.org/isoiec-27001-information-security.html> accessed 10 April 2022

Lloyd's, 'Cyber Risks & Exposures : Market Bulletin Ref : Y4842' (25 November 2014) <https://assets.lloyds.com/assets/y4842/1/Y4842.pdf > accessed 18 September 2022

Lloyds Maritime Law Newsletter, 'London Arbitration 25/19' (07 November 2019, Informa)

Lloyd's, 'Performance Management – Supplemental Requirements & Guidance' (July 2020) <https://assets.lloyds.com/assets/performance-management-supplemental-requirements-and-guidance-july-2020highlighted/1/Performance%20Management%20Supplemental%20Requirements%20and%20Guidance%20July%202020Highlighted.pdf> accessed 18 September 2022

Lloyds, 'Providing clarity for Lloyd's customers on coverage for cyber exposures (Market Bulletin Y5258)' (4 July 2019) <https://www.lloyds.com/news-and-insights/market-communications/market-bulletins/?Query=Y5258&Filters=%5B%5D&OrderBy=&Page=1&StartDate=&EndDate=&Type=MarketBulletin&DateChanged=false&HideFields=> accessed 18 September 2022

Lloyd's Register, 'Cyber Security BIMCO Guidelines: Assessing compliance to the BIMCO guidelines' (2020) <https://www.lr.org/en/bimco-guidelines/> accessed 18 September 2022

LMA, 'Cyber War and Cyber Operation Exclusion Clauses' (LMA21-042-PD, 25 November 2021) <https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx> accessed 18 September 2022

Lund H S, 'Handbook on Loss of Hire Insurance' (Norwegian Hull Club, 3rd edn. 2016) <https://www.norclub.com/casualty-response/loss-of-hire?a=Introduction> accessed 18 September 2022

Newman R, 'Cyber pirates terrorising the high seas' (IET, 18 April 2019) <https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/> accessed 18 September 2022

NCSC, ‘Guidance: Mitigating malware and ransomware attacks’ (Version 3.0, 09 September 2021) <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks> accessed 18 September 2022

North, ‘FAQS: General Data Protection Regulation (GDPR) (January 2018) < https://www.nepia.com/search?q=gdpr+faqs> accessed 24 September 2022

Marsh, ‘Piracy – Insurance Implications’ (2011) <https://static.mycoracle.com/igpi_website/media/article_attachments/Marsh%20Piracy%20implications.pdf> accessed 18 September 2022

Monero, ‘RingCT’ (Muneropedia, 2022) <https://www.getmonero.org/resources/moneropedia/ringCT.html> accessed 18 September 2022

Monero, ‘Ring signature’ (Moneropedia, 2022) <https://www.getmonero.org/resources/moneropedia/ringsignatures.html> accessed 18 September 2022

Monero, ‘Stealth Address’ (Moneropedia, 2022) <https://www.getmonero.org/resources/moneropedia/stealthaddress.html> accessed 24 September 2022

Oxford English Dictionary (OUP 2019) <https://www.lexico.com/en/definition/force> accessed 18 September 2022

Paton A, ‘Hull Clauses and Claims - time for some marriage counselling?’ (The Association of Average Adjusters Chairman’s Address, 12 May 2016) <https://issuu.com/assocavgadj/docs/association_of_average_adjusters_an> accessed 18 September 2022

P&I, ‘Revised Piracy – FAQs: Revised December 2019’ <https://www.igpandi.org/article/piracy-faqs-revised-december-2019> accessed 18 September 2022

PWC, ‘Putting a Value on Data’ (2019) <https://www.pwc.co.uk/data-analytics/documents/putting-value-on-data.pdf> accessed 24 September 2020.

RSA Insurance plc, ‘Cyber Risk Insurance Policy Wording’ (UKC05268A September 2018) <https://www.rsainsurance.co.uk/media/ruhfu0rp/cyber-risk-insurance-policy-wording-ukc05268a.pdf > accessed 18 September 2022

Seafarers: High Resolution’ (Witherby Publishing, June 2018)

<https://www.maritimeglobalsecurity.org/media/1040/global-counter-piracy-guidance-bmp_high_01-04-19.pdf> accessed 18 September 2022

SIGCo Group, 'Cyber Hull Insurance' (v4- 21 July 2021)
< https://www.sigcogroup.com/docs/Policy_Wording_Revised_v1.4.pdf> accessed 18 September 2022

Silver P, 'Stuck in the doldrums? A consideration of whether the ABS Loss of Charter Hire Insurance wording is still fir for purpose' (The Association of Average Adjusters Chairman's Address, 10 May 2012)
<https://docshare.tips/aaa-chairmans-address-on-loh_587ee6a3b6d87fb5398b58f4.html > accessed 18 September 2022

Standard Club, 'Rule Book 2022/23 P&I Rules' (2022)
< https://www.standard-club.com/rules/rules-2022-2023/> accessed 24 September 2022

The London P&I Club, 'Class 5 The Protecting and Indemnity Rule 2022/ 2023' (2022)
<https://www.londonpandi.com/documents/the-london-club-pplusi-rules-class-5-2022-2023/> accessed 18 September 2022

The Nordic Association of Marine Insurers and others, 'The Nordic Marine Insurance Plan of 2013, Version 2019' <http://www.nordicplan.org/The-Plan/Part-Three/Chapter-16/#Clause-16-1> accessed 18 September 2022

The U.S. Department of the Treasury's Office, ' Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments' (OFAC, 01 October 2020)
< https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf> accessed 18 September 2022

Tokio Marine HCC, 'Professional Risks Cyber Security Policy Wording 0417' (October 2017)
<https://www.tmhcc.com/-/media/RoW/Documents/PI/Cyber/Cyber-Security-Insurance-Wording-0417.pdf >accessed 24 September 2022.

UK Jurisdiction Taskforce, 'Legal statement on cryptoassets and smart contracts' (November 2019) <https://technation.io/lawtech-uk-resources/#cryptoassets> accessed 18 September 2022

UK P&I, 'Rules 2022' (2022) <https://www.ukpandi.com/news-and-resources/rulebook-2022?chapter=conditions+exceptions+and+limitations> accessed 18 September 2022

US Department of Justice, 'Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research' (Office of Public Affairs, 21

July 2020) < https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion> accessed 27 September 2022.

US Department of Justice, 'Two Chinese Hackers Associated with Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information' (Office of Public Affairs, 20 December 2018) < https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion> accessed 27 September 2022.

Ziolkowski K, 'Stuxnet – Legal Considerations' (CCDCOE 2012) <https://ccdcoe.org/uploads/2018/10/Ziolkowski_Stuxnet2012-LegalConsiderations.pdf> accessed 18 September 2022

Zurich Insurance plc, 'Cyber Policy' SME513C.04 (NP721418004) (10/20) CMS <https://www.zurich.co.uk/business/business-insurance/specialty-lines/financial-lines/cyber> accessed 24 September 2022.