CyRiM Report 2019

Shen attack
Cyber risk in Asia Pacific ports

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE
LLOYD'S
AON Empower Results®
MSIG
SCOR The Art & Science of Risk
TransRe We value risk.
Centre for Risk Studies
UNIVERSITY OF CAMBRIDGE Judge Business School

About CyRiM

Cyber risks are emerging risk with new complexities that call for insurers and risk managers to jointly develop innovative solutions and tools and enhance awareness and underwriting expertise.

The Cyber Risk Management (CyRiM) project is led by NTU-IRFRC in collaboration with industry partners and academic experts. CyRiM is a pre-competitive research project that aims to foster an efficient cyber risk insurance market place through engaging industry and academic experts guided by government and policy level research. The CyRiM project will help Singapore become an industry centre of excellence on cyber risk and grow the cyber risk insurance market by promoting both the demand and the supply of insurance coverage.

For more information about CyRiM please visit
http://irfrc.ntu.edu.sg/Research/cyrim/Pages/Home.aspx

CyRiM disclaimer

This report has been co-produced by Lloyd's, Aon, MSIG, SCOR, TransRe and CyRiM for general information purposes only. This does not reflect the views of the Nanyang Technological University of Singapore Insurance Risk and Finance Research Centre and additionally does not necessarily reflect the views of any CyRiM partners. While care has been taken in gathering the data and preparing the report and the information herein, Lloyd's, CyRiM, the Nanyang Technological University of Singapore Insurance Risk and Finance Research Centre and the Cambridge Centre for Risk Studies do not make any representations or warranties as to its accuracy or completeness and expressly excludes to the maximum extent permitted by law all those that might otherwise be implied. Lloyd's, Aon, MSIG, SCOR, TransRe, the Nanyang Technological University of Singapore Insurance Risk and Finance Research Centre, CyRiM and the Cambridge Centre for Risk Studies accept no responsibility or liability for any loss or damage of any nature occasioned to any person as a result of acting or refraining from acting as a result of, or in reliance on, any statement, fact, figure or expression of opinion or belief contained in this report. This report does not constitute advice of any kind.

About Cambridge Centre for Risk Studies

The Centre for Risk Studies is a world leading centre for the study of the management of economic and societal risks. The Centre's focus is the analysis, assessment, and mitigation of global vulnerabilities for the advancement of political, business, and individual decision makers.

The Centre provides frameworks for recognizing, assessing, and managing the impacts of systemic threats. The research programme is concerned with catastrophes and how their impacts ripple across an increasingly connected world with consequent effects on the international economy, financial markets, firms in the financial sectors, and global corporations. To test research outputs and guide new research agendas, the Centre engages with the business community, government policy makers, regulators, and industry bodies.

Cambridge Centre for Risk Studies disclaimer

This report describes a hypothetical scenario developed as a stress test for risk management purposes. It is not a prediction. The Cambridge Centre for Risk Studies develops hypothetical scenarios for use in improving business resilience to shocks. These are contingency scenarios used for 'what-if' studies and do not constitute forecasts of what is likely to happen.

The views contained in this report are entirely those of the research team of the Cambridge Centre for Risk Studies, and do not imply any endorsement of these views by the organisations supporting the research, or our consultants and collaborators. The results of the research presented in this report are for information purposes only. This report is not intended to provide a sufficient basis on which to make an investment decision. The Centre is not liable for any loss or damage arising from its use. Any commercial use will require a license agreement with the Cambridge Centre for Risk Studies.

Key contacts

Trevor Maynard
Head of Innovation, Lloyd's
trevor.maynard@lloyds.com

Shaun Wang
Project Lead, CyRiM
shaun.wang@ntu.edu.sg

For general enquiries about this report and Lloyd's work on emerging risks, please contact
innovation@lloyds.com

Cambridge Centre for Risk Studies

Research team:
- Dr Jennifer Daffron, Research Associate
- Kelly Quantrill, Research Assistant
- Jennifer Copic, Research Associate
- Kayla Strong, Research Assistant
- Simon Ruffle, Director of Research and Innovation
- Dr Andrew Coburn, Director of Advisory Board
- Timothy Douglas, Research Assistant
- Eireann Leverett, Senior Risk Researcher
- James Bourdeau, Research Assistant
- Oliver Carpenter, Research Assistant
- Tamara Evan, Research Assistant
- Ken Deng, Research Assistant
- Professor Danny Ralph, Academic Director
- Dr Michelle Tuveson, Executive Director

Report citation:

Lloyd's of London, Cambridge Centre for Risk Studies, and Nanyang Technological University, *Shen attack: Cyber risk in Asia Pacific ports*, 2019

Or

Daffron, J., Ruffle, S., Coburn, A., Copic, J., Quantrill, K., Strong, K., Leverett, E., Cambridge Centre for Risk Studies, *Shen attack: Cyber risk in Asia Pacific ports*, 2019

Insurance industry interviews and consultation
- Ed Messer, Aon
- Andrew Mahony, Aon
- Lauren Clarke Wiest, Aon
- Alan Godfrey, Axis Capital
- Joe Mellen, Antares
- John Moore, Delta Insurance
- Jasper Hartono, Delta Insurance
- Matt Harrison, Hiscox
- Kara Owens, Markel
- Guenter Kryszon, Markel
- John Brice, MSIG
- Lucien Mounier, Beazley
- Sebastien Heon, SCOR
- Grace Lim, TransRe
- Rhett Hewitt, TransRe
- Lauren Markowski, TransRe

Lloyd's project team
- Dr Trevor Maynard, Innovation
- Anna Bordon, Innovation
- Kieron Price, Innovation
- Angela Kelly, Commercial
- Pavlos Spyropoulos, Commercial
- May Chen, Commercial
- Amy Fu, Commercial
- Linda Miller, Global Marketing
- Sharonjeet Meht, Global Marketing
- Flemmich Webb, External Communications
- Nathan Hambrook-Skinner, External Communications
- Albert Kuller, Class of Business
- Guy Sellers, Class of Business
- Christian Stanley, Class of Business
- Chris Murlowski, Class of Business

Lloyd's Market Association
- Patrick Davison, Deputy Director, Underwriting
- Phil Norwood, Senior Executive, Underwriting
- Tony Elwood, Senior Executive, Underwriting
- Gary Budinger, Senior Executive, Finance and Risk

Nanyang Technological University – Insurance Risk and Finance Research Centre (NTU-IRFRC)
The Centre is established at the Nanyang Business School (NBS), Nanyang Technological University, Singapore. It aims to promote insurance and insurance related risk research in the Asia Pacific. It is seen as a key foundation to establishing dialogue between the industry, regulators and institutions, and sharing critical knowledge to facilitate the growing role of the insurance industry in the economic development of the region.

Further thanks go to the remaining cyber experts who wish to remain anonymous.

About CyRiM

The Cyber Risk Management (CyRiM) project is led by Nanyang Technological University – Insurance Risk and Finance Research Centre (NTU-IRFRC) in collaboration with industry partners and academic experts including the Cambridge Centre for Risk Studies. CyRiM is a pre-competitive research project that aims to foster an efficient cyber risk insurance market place through engaging industry and academic experts guided by government and policy level research. The CyRiM project will help Singapore become an industry centre of excellence on cyber risk and grow the cyber risk insurance market by promoting both the demand and supply of insurance coverage.

Scope

The project initially considered all cyber related insurance risks such as data breach, property damage, personal injury and loss of life, liability, reputation damage, infrastructure damage, and terrorism. However, for effective data analytics, the project's scope was refined through identification and selection of those risks considered insurable and suitable for further actuarial modelling. The full range of risks are considered in the cyber event scenarios.

The CyRiM project is based in Singapore and has a strong focus on building local capabilities relating to cyber risk while also maintaining a global perspective with hubs in the US and Europe.

Problem statement

The real and present danger posed by cyber risk to businesses and society needs to be tackled on multiple levels. Insurance is one important component in managing this rapidly growing threat as it can provide risk mitigation and transfer. However, the insurance industry is improving the understanding of the unique, complex and evolving nature of cyber risk to provide a robust cyber insurance cover required by those at risk.

The lack of sound data, the rapidly changing cyber threat environment, developing regulation and policy landscape, and the global nature of cyber risk with potential for high accumulation risk, constrains the development of the current cyber risk insurance market.

Objectives

- Research into the definition of cyber risk with the aim of delivering an appropriate classification that also considers the emerging cyber information risk landscape and jurisdiction variations.
- Creation of a cyber related event loss data-set including analysis of risk drivers and translation to estimated insurance claims based on a standardised set of defined contract wordings.
- Creation of a set of cyber event scenarios for impact quantification and study of accumulation risk in systemic events.
- Creation of benchmark cyber loss models and dependency information to support actuarial pricing.
- Collaborative development of a non-intrusive cyber security exposure assessments capability to support company rating and integration with underwriting processes.

Governance and funding

- Aon
- Lloyd's of London
- MSIG
- SCOR
- TransRe

The project is overseen by a Project Oversight Board consisting of representatives of Monetary Authority of Singapore (MAS), Cyber Security Agency of Singapore (CSA), NTU-IRFRC and the industry Founding Members.

Executive summary

What would the impact be on the global economy and insurers if several ports in Asia-Pacific were forced to close as a result of a cyber-attack?

This report seeks an answer to this question by exploring the impact of a hypothetical computer virus, Shen - from the Chinese mythological clam monster, used maliciously against a port management system which closes up to 15 ports across several Asia-Pacific countries.

While cyber-attacks have impacted individual ports in the past, an attack on systemic vulnerabilities across ports on this scale has never been seen. However, the combination of aging shipping infrastructure and globally complex supply chains, makes the shipping industry vulnerable to extreme losses. This attack takes advantage of a vulnerability in port management software provided by a prominent hypothetical ship management company, which manages hundreds of ships.

The narrative of this attack is especially useful because it reveals the complex marine cargo management supply chain and exposes the potential threat posed by insecure third-party suppliers.

The scenario presents three variants of increasing losses, with all results reflecting low probability, high impact situations. The S1 scenario variant affects ports located in Japan, Malaysia, and Singapore. The S2 scenario variant adds The Republic of Korea to the affected countries of S1. The X1 scenario variant adds China, the world's largest shipping export country, to the affected countries in the previous variants for a total of 15 ports affected.

Box 1: Key findings

- Economic damage to the world economy from a concerted global cyber-attack on 15 Asian ports may range from between $40.8 billion (in the least severe scenario variant, S1) to $109.8 billion (in the most severe scenario variant, X1).
- The sectors that suffer the heaviest direct and indirect economic losses are Transportation / Aviation / Aerospace, Retail, Manufacturing, and Real Estate / Property / Construction.
- Productivity losses affect each country that has bilateral trade with the attacked ports. Asia would be the worst affected region, set to lose up to $26bn in indirect economic losses, followed by $623m in Europe and $266m in North America.
- The total claims paid by the insurance industry is estimated at $3.6 billion for S1 to $8.3 billion for X1.
- Insurance industry losses are between 8% and 9% of the total economic loss, which shows there are high levels of underinsurance for this type of cyber-attack.
- Business Interruption and Contingent Business Interruption coverages are the main drivers of the insured losses (63% of total losses for S1, 60% for X1).
- Non-affirmative cyber, meaning that cyber is not explicitly mentioned in the policies, accounts for 62% of the total insured losses in S1 and 57% in X1.
- In scenario variant X1 port operators will carry 50% of the insured losses.

Table 1: Economic losses from the hypothetical Shen attack on port management systems in the Asia-Pacific region by scenario variant

Scenario variant	Countries with ports directly affected	Number of ports affected	Total economics losses ($bn)	Direct economic losses ($bn)	Indirect Economic losses ($bn)
S1	Japan, Malaysia, Singapore	6	$40.8	$25.7	$15.1
S2	Japan, Malaysia, Singapore, The Republic of Korea	9	$55.9	$36.8	$19.1
X1	Japan, Malaysia, Singapore, The Republic of Korea, China	15	$109.8	$83.7	$26.1

Values have been rounded to the nearest whole number.

This is a deterministic scenario. The University of Cambridge Centre for Risk Studies (CCRS) is not attempting to put uncertainty or probability to the values presented in this report. A series of events is assumed, for which specific outcomes are assigned. The detailed loss estimates shown are a result of the granularity of the calculation process. Figures presented are potential estimates, not the projected outcome. This is an appropriate approach for a deterministic outlook involving multiple threats in a clash event.

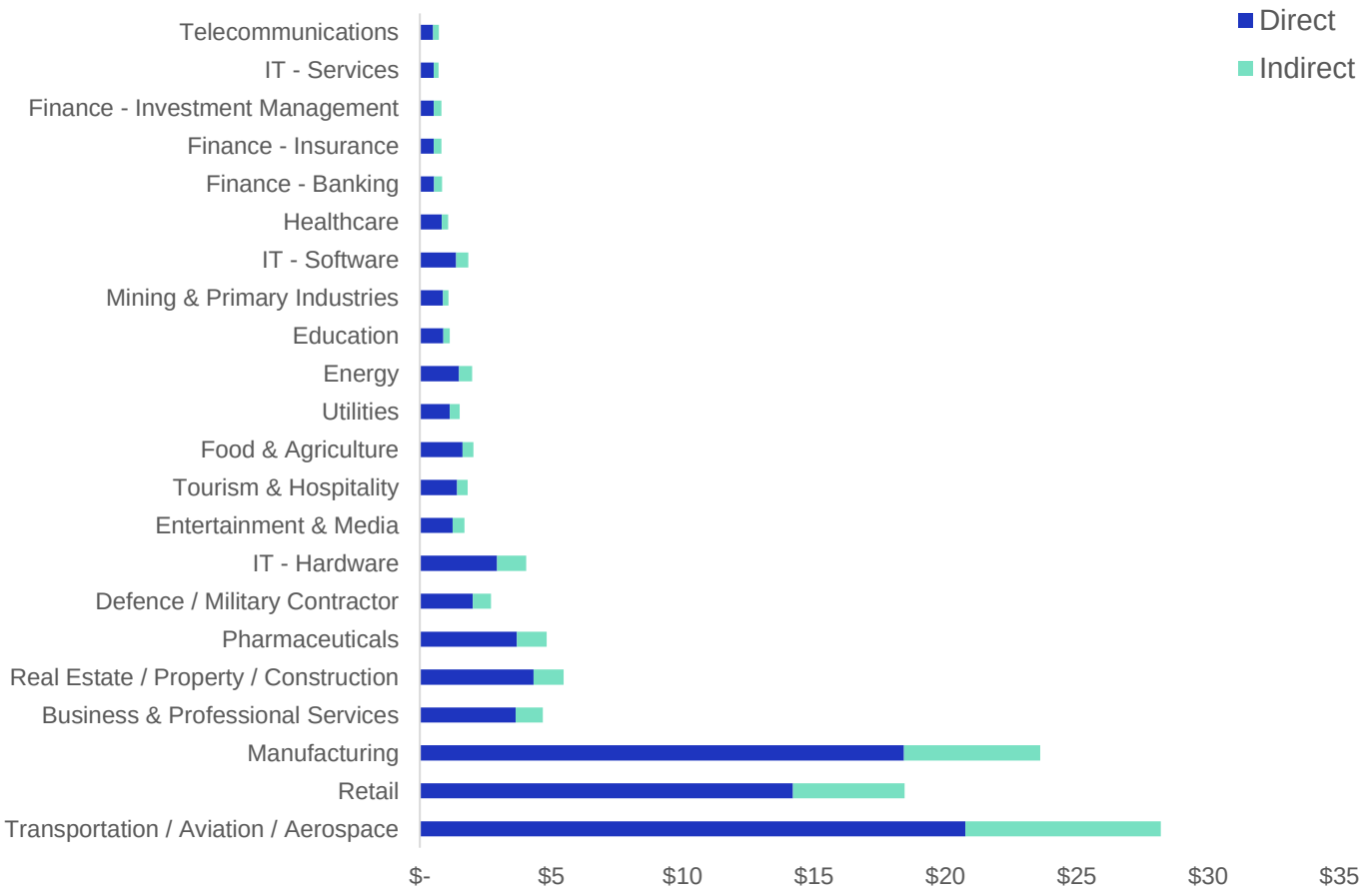
For the purposes of this scenario, ports in the Asia-Pacific are no more vulnerable to the Shen virus than ports in other parts of the world. Asian ports are affected, and these impacts are modelled, because they are targeted directly by the Shen virus. If the attackers had chosen to focus their efforts on ports in the United States, for example, then similar vulnerabilities and impacts would be seen, but insurance losses could be higher in certain classes.

'Shen attack: Cyber risk in Asia Pacific ports' is the second of two joint reports produced by the Cyber Risk Management (CyRiM) project led by Nanyang Technological University, in collaboration with industry partners and academic experts including the Cambridge Centre for Risk Studies. CyRiM industry founding members include Aon, Lloyd's - the specialist insurance and reinsurance market, MSIG, SCOR, and TransRe.

Economic losses by industry sector and countries

The scenario shows the economic damage to the world economy from a concerted global cyber-attack on 15 Asian ports may range from between $40.8 billion (in the least severe scenario variant, S1) to $109.8 billion (in the most severe scenario variant, X1).

Figure 1: Total global direct and indirect economic losses by sector for scenario variant X1



Direct economic losses

Economic losses mount from direct losses due in part to perishables and delayed delivery of goods, with most of the losses stemming from business interruption from port closures. Indirect losses flow through the global maritime supply chain reaching across the world. All sectors are impacted by the scenario, but the sectors that suffer the heaviest direct and indirect economic losses are Transportation / Aviation / Aerospace, Retail, Manufacturing, and Real Estate / Property / Construction. These sectors are heavily reliant on economic input from the Transportation sector. The impacts from port closures will be global.

- Port closures in Japan will directly affect the USA, China, the Republic of Korea, the Republic of China (ROC) and Hong Kong Special Administrative Region of the People's Republic of China. In 2017, 32% of Japan's exports to the USA were cars and 7.2[1]% of their exports to China were electronic integrated circuits, indicating a significant impact to the Manufacturing sector in these trade partner countries.
- Malaysia's top maritime trading partners, Singapore, China, the USA, Japan, and Thailand will be adversely affected by any restriction to day-to-day shipping functions.
- The closure of the port in Singapore will affect China, Hong Kong Special Administrative Region of the People's Republic of China, Malaysia, the USA, and Indonesia. In 2017 Singapore's primary exports to China were predominantly electronic integrated circuits (40%) and refined petroleum oils (7.5%),[2] so Manufacturing and IT - Hardware will suffer severely in this scenario.

[1] The Observatory of Economic Complexity 2017

[2] The Observatory of Economic Complexity 2017

- Ports' shutdown in The Republic of Korea will have a significant impact to their top five exporting markets of China, USA, Vietnam, Hong Kong Special Administrative Region of the People's Republic of China, and Japan. 31% of their exports to China in 2017[3] were electronic integrated circuits, so any constraints placed on the shipment of these goods would have negative implications for the Manufacturing sector in particular.
- The international reach of port closures in China will be experienced throughout the world with the countries of USA, Hong Kong Special Administrative Region of the People's Republic of China, Japan, The Republic of Korea, and Vietnam suffering highest direct losses from the closures.

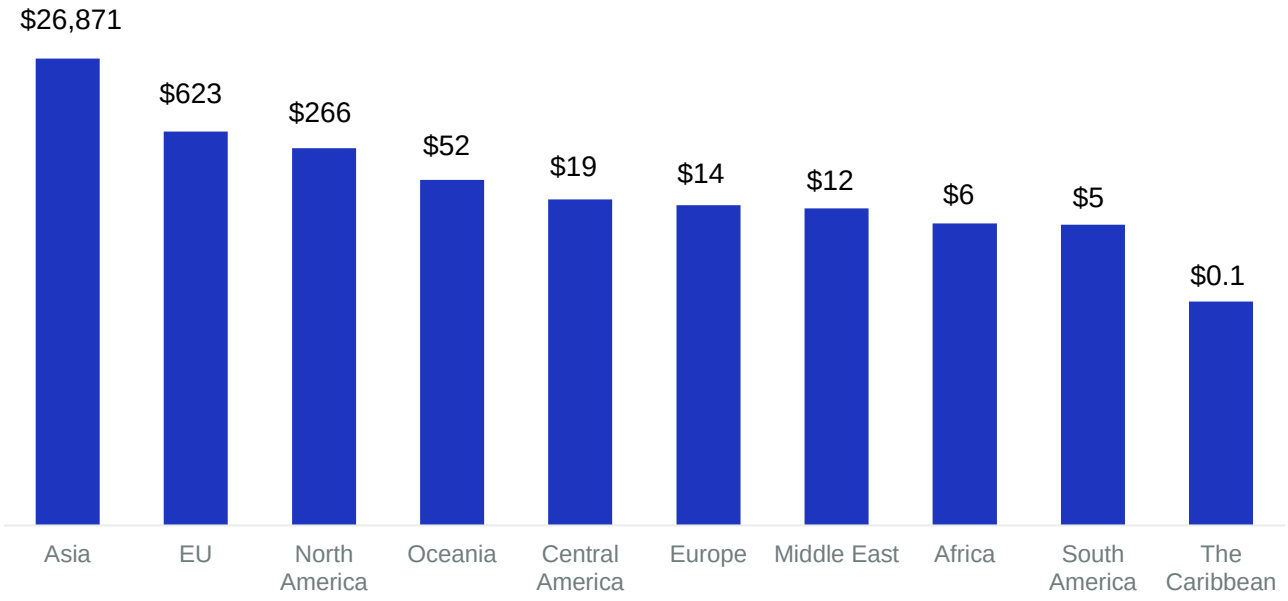
Indirect economic losses

Although the Shen virus only directly affects ports in the Asia Pacific region, economic losses are felt around the world from this scenario due to the global nature of the maritime supply chain.

The indirect losses modelled in this scenario are the productivity losses for each country that has bilateral trade with the affected ports in their respective countries. A daily loss is calculated for each affected country based on the GDP, merchandise trade, world container share percentage, country exports,[4] and bilateral trade index of the 155 countries for which data is available.[5]

Productivity losses affect each country that has bilateral trade with the attacked ports. Asia would be the worst affected region, set to lose up to $110bn in indirect economic losses, followed by $816m in Europe and $348m in North America.

Figure 2: Total indirect losses by region ($million)



In this figure a logarithmic scale is applied to account for the large differences across territories.

The indirect losses presented in this report are cautious estimates. Though they have been modelled extensively, they are not modelled through all levels of the supply chain. For example, the direct impact to ports in China is expected to impact the US economy. This has been modelled and these losses are included in the report. However, the tertiary impact that the impact to the US economy has is not modelled. As a result, the indirect losses shown here can foreseeably be significantly higher as the impacts compound through multiple supply chain tiers.

[3] The Observatory of Economic Complexity 2017
[4] World Integrated Trade Solution 2017
[5] UNCTADstat 2018a

Insurance losses

The report also analyses the implications of these direct and indirect consequences on insurance losses. The scenario shows that during and after such an attack insurance claims would be made for Business Interruption, Contingent Business Interruption, Directors and Officers, Marine Cargo, Technology Errors and Omissions, Regulatory and Defence Coverage, Data and Software Loss, Incident Response costs and Reputational Risk. Notably, not all jurisdictions or insurers recognise data as property. Losses highlighted in this report may vary and policyholders should always check with their insurer definitions and exclusions.

The total claims paid by the insurance industry is estimated at $3.6 billion for S1 to $8.3 billion for X1. Comparing the insurance loss estimates to the economic losses shows insurance industry losses are between 8% and 9% of the total economic loss, which shows there are high levels of underinsurance for this type of cyber-attack. This is driven by low levels of cyber insurance penetration and policy limit structures that were frequently unable to support the scale of losses modelled in this scenario. Close examination of these results indicates that Business Interruption and Contingent Business Interruption (CBI) coverages are the main drivers of the insured losses (63% of total losses for S1, 60% for X1). In this report, indirect economic losses are estimated at a country level via supply chain impacts, focusing on countries with close trading relationships to the affected countries. This loss then flows into an insurance model of the level of CBI coverage available within each country. CBI insurance is complex and challenging to model, further research on the topic is required.

Table 2: Total economic and insurance losses by scenario variant

Scenario variant	Countries	Total economic losses ($bn)	Insured losses ($bn)	Uninsured losses ($bn)	Insurance loss as a % of economic loss
S1	Japan, Malaysia and Singapore	$40.8	$3.6	$37.2	8.8%
S2	+ The Republic of Korea	$55.9	$4.9	$60	8.9%
X1	+ China	$109.8	$8.3	$101.6	7.5%

Values have been rounded to the nearest whole number.

Affirmative' and 'non-affirmative' cyber insurance losses

The report also analyses the impacts of the scenario on 'affirmative' and 'non-affirmative' cyber insurance losses (standalone cyber policies and cyber endorsements on traditional policies are considered affirmative cyber insurance, while traditional policies without explicit exclusions are considered non-affirmative).

The scenario shows that during and after such an attack insurance claims would be made for Business Interruption, Contingent Business Interruption, Reputation Risk, Incident Response Costs, Regulatory Defence Coverages, and Liability risks. Non-affirmative cyber accounts for 62% of the total insured losses in S1 and 57% in X1. Port Management System and Ship Owners will see all their losses (7% of the total) from non-affirmative cyber.

Types of companies that would make claims

These are the primary categories of policyholders that would make claims in this scenario:

– Port Operators

- Port Operators are defined as companies or boards who regulate and manage port and marine services, facilities, and activities within their associated jurisdictional waters.
- In scenario variant X1 port operators will carry 50% of the total insured losses of which 63% will be under an All Risks policy (non-affirmative cyber).

– Third-Party Organizations Indirectly Impacted

- Third-party organizations who are indirectly impacted include those who are impacted further along the supply chain.
- In scenario variant X1, Third-Party Organizations Indirectly Impacted (Supply Chain Companies) will carry 21% of the total insured losses of which 89% will be under an All Risks policy (non-affirmative cyber).

– Logistics and Cargo Handling Companies

- Logistics and Cargo Handling Companies are responsible for the planning, execution and control of the movement of cargo and goods, information, and services. Logistics and Cargo Handling Companies connect the marine cargo industry with wider supply chains.
- In scenario variant X1 Logistics and Cargo Handling Companies will carry 16% of the total insured losses of which 65% will be under an All Risks policy (non-affirmative cyber).

– Perishable Cargo Content Owners

- The cargo content owners are either individuals or organisations that have paid for cargo under a legal contract. It is assumed that roughly 7% of the cargo turnover is perishable and has spoilage due to shipping delays.
- In scenario variant X1 cargo content owners will carry 3% of the total insured losses, all affirmative.6

– Ship Owners

- Ship owners are the individuals or organisations responsible for the ownership and operation of the vessel.
- In scenario variant X1 ship owners will bear less than 1% of the total insured losses, all non- affirmative.

– Port Management System

- The Port Management System is a software application that supports the administration and operations of port operators in a range of tasks.
- In scenario variant X1 port operators will carry 6% of the total insured losses, all non- affirmative

– Ship Management Company

- A Ship Management Company is a company independent of the owner of the ship which maintains and operates the vessel.
- In scenario variant X1 the Ship Management Company will carry 3% of the total insured losses of which 87% will be under an All Risks policy (non-affirmative cyber).

Conclusions

The maritime supply chain is a complex system of interconnected economies. There is no doubt that technology has improved the shipping industry allowing for better tracking, management, and just-in-time deliveries, however, aging ships are a problem. Many vessels at sea are over thirty years old and were not designed with cyber in mind. Responding to these challenges is therefore critical for the well-being of the maritime industry and those who insure it.

Many sectors would be affected across the world with the largest losses arising from the Transportation / Aviation / Aerospace, Retail, Manufacturing, and Real Estate / Property / Construction sectors. This report highlights the current insurance gap for the marine industry where 92% of the economic losses in the extreme version of the scenario are uninsured. Finally, systemic cyber vulnerabilities can have a catastrophic effect on the global supply chain, stemming from the directly affected country or sector with contingent business interruption identified as particularly damaging.

However, there are also opportunities for insurers to grow their business in the insurance classes associated with the Shen Attack scenario. For example, Asia is one of the fastest-growing markets for cyber insurance. The market saw an 87% increase in cyber insurance take-up rates in Asia in 2017 with the current global premiums estimated to total $50 million.[7] The increase in cyber-attacks in 2017 in Asia over recent years means companies are more likely to have standalone cyber insurance than before, although with low sub-limits and more limited take-up of first party BI coverage when compared to other markets. Further insurance take-up is likely in the future for directors and officers (D&O) policies as changes in the business environment as such tight corporate governance and new regulations are introduced.

The expansion of the cyber insurance market is both necessary and inevitable. Scenarios such as the 'Bashe Attack' and the 'Shen Attack' will help insurers and policyholders to expand their view of cyber risks ahead of the next event and help them create new products, services and mitigation strategies that make businesses and communities more resilient. To achieve this continuing the collection and sharing of quality cyber-attack data is an important element that will enable technological and insurance solutions required for cyber risks that are constantly changing.

[6] Strictly speaking no affirmative standalone cyber cover or endorsement for Cargo is available. A notable exclusion in the Marine insurance industry is the Institute Cyber Attack Exclusion Clause (CL380). CL380 excludes insurance cover for risks occurring because of cyber-attacks. Within this scenario, marine policies are assumed to have a 50% exclusion rate to account for CL380.

[7] Williams 2016; Weinland 2017; OECD 2017

References

OECD. 2017. “Enhancing the Role of Insurance in Cyber Risk Management.” OECD Publishing, Paris, 142. http://dx.doi.org/10.1787/9789264282148-en.

The Observatory of Economic Complexity. 2017. “Products Exported by China 2017.” The Observatory of Economic Complexity. 2017. http://atlas.media.mit.edu/en/visualize/tree_map/hs92/export/chn/all/show/2017/.

UNCTADstat. 2018a. “Liner Shipping Bilateral Connectivity Index, Annual.” 2018. https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=96618.

Weinland, Don. 2017. “AIG Reports 87% Rise in Asia Cyber Insurance Requests.” Financial Times, August 9, 2017. https://www.ft.com/content/6362bc1a-2af4-3442-b461-f679174bc72d.

Williams, Ann. 2016. “Demand for Cyber Insurance in Singapore to Grow by 50% in 2016: AIG.” The Straits Times, March 31, 2016. http://www.straitstimes.com/business/banking/demand-for-cyber-insurance-in-singapore-to-grow-by-50-in-2016-aig.

World Integrated Trade Solution. 2017. “Trade at a Glance: Most Recent Values.” World Integrated Trade Solution. 2017. https://wits.worldbank.org/countrysnapshot/en/CHN.

CyRiM Report 2019

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE
LLOYD'S
AON Empower Results®
MSIG
SCOR The Art & Science of Risk
TransRe We value risk.
Centre for Risk Studies
UNIVERSITY OF CAMBRIDGE Judge Business School